

Exhibit “B”

BOIES SCHILLER FLEXNER LLP

David K. Willingham SBN 198874
dwillingham@bsfllp.com
725 S Figueroa Street
Los Angeles, California 90017
31st Floor
Phone: (213) 629-9040
Fax: (213) 629-9022

Amy L. Neuhardt (*pro hac vice*)
aneuhardt@bsfllp.com
1401 New York Avenue, NW
Washington, DC 20005
Phone: (202) 237-2727
Fax: (202) 237-6131

Lee S. Wolosky (*pro hac vice*)
lwolosky@bsfllp.com
Robert J. Dwyer (*pro hac vice*)
rdwyer@bsfllp.com
575 Lexington Ave., 7th Floor
New York, NY 10022
Phone: (212) 446-2300
Fax: (212) 446-2350

Counsel for Plaintiffs

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION**

BROIDY CAPITAL MANAGEMENT
LLC and ELLIOTT BROIDY,

Plaintiffs,

v.

STATE OF QATAR, STONINGTON
STRATEGIES LLC, NICOLAS D.
MUZIN, GLOBAL RISK ADVISORS
LLC, KEVIN CHALKER, DAVID
MARK POWELL, MOHAMMED BIN
HAMAD BIN KHALIFA AL THANI,
AHMED AL-RUMAIHI, and DOES 1-
10,

Defendants.

Case No. 18-cv-02421-JFW

**FIRST AMENDED COMPLAINT
AND DEMAND FOR JURY TRIAL**

The Honorable John F. Walter

1 Plaintiffs Broidy Capital Management LLC (“BCM”) and Elliott
2 Broidy (“Broidy”), by and through their attorneys Boies Schiller Flexner LLP,
3 bring this action seeking injunctive relief and monetary damages against
4 Defendants the State of Qatar, Stonington Strategies LLC (“Stonington”),
5 Nicolas D. Muzin (“Muzin”), Global Risk Advisors LLC (“GRA”), Kevin
6 Chalker (“Chalker”), David Mark Powell (“Powell,” and together with
7 Chalker and GRA the “GRA Defendants”), Mohammed bin Hamad bin
8 Khalifa al Thani (“Al Thani”), Ahmed al-Rumaihi (“Al-Rumaihi,” and
9 together with al Thani and the State of Qatar, the “Qatari Defendants”), and
10 Does 1-10, for Defendants’ unlawful conduct, as set forth below.¹

11 NATURE OF THE ACTION

12 1. This case presents the issue of whether a nation state can
13 orchestrate and execute a criminal conspiracy directed against a United States
14 citizen on United States soil and then invoke sovereign immunity to avoid
15 liability, accountability and exposure.

16 2. Defendant State of Qatar reacted after neighboring Middle
17 Eastern countries sanctioned, embargoed and isolated Qatar commercially and
18 diplomatically in June 2017 for its support of terrorist organizations, and after
19 Qatar’s subsequent shunning by President Trump, by launching a wide-
20 ranging and extremely well-resourced effort to influence public opinion in the
21 United States. Defendants Al Thani and Al-Rumaihi, a Qatari operative
22 present in the United States, were the architect of these efforts, which included
23 (among other things) initiatives to attack and discredit those who had spoken
24
25

26 ¹ The GRA Defendants, Does 1-10 and Defendants Muzin, Stonington and Al-
27 Rumaihi, are sometimes referred to herein as the “Agent Defendants.”

1 out against Qatar, and – according to court documents – efforts to bribe
2 individuals close to President Trump.

3 3. Defendant State of Qatar (which as a principal is bound by the
4 actions and knowledge of its agents) hired numerous United States agents at a
5 cost of millions of dollars, including by entering into specific agreements with
6 those agents for those agents to provide public relations, consultancy, and
7 related services. Some of those agents disclosed their work for Qatar by
8 making filings pursuant to the Foreign Agents Registration Act (such as
9 Defendants Stonington and Muzin) while others worked secretly for the State
10 of Qatar and did not make filings (such as Joseph (“Joey”) Allaham and the
11 GRA Defendants).

12 4. In late 2017, the whitewashing campaign organized by Al Thani
13 and Al-Rumaihi – on behalf of and with the knowledge of and agreement to
14 by Defendant State of Qatar – was encountering serious problems and targeted
15 Plaintiff Broidy. Plaintiff Broidy’s public and private actions and statements
16 stood in the way of the State of Qatar’s aggressive public relations and
17 governmental relations efforts that sought to ingratiate Qatar with the new
18 Trump Administration and to deflect attention from Qatar’s record of
19 supporting terrorist organizations.

20 5. On information and belief, Defendant Chalker is a former CIA
21 cyber-operative who runs GRA, which is headquartered in New York, New
22 York. On information and belief, Defendant Powell is a former British
23 intelligence operative who runs GRA operations out of Qatar and established
24 GRA’s office there through a Gibraltar subsidiary in October 2017 – just
25 weeks prior to the commencement of the attack on Plaintiffs.

26 6. On information and belief, the Qatari Defendants retained and
27 used the GRA Defendants to coordinate and implement the hack, and the
28

1 GRA Defendants also personally supervised aspects of the information
2 operation against Plaintiffs.

3 7. On information and belief, the GRA Defendants introduced
4 Defendant State of Qatar to cyber mercenaries in various countries to
5 coordinate technical aspects of the illegal intrusion into Plaintiffs' email
6 server in Los Angeles and Google LLC's server(s) in California, and the
7 dissemination of the contents to U.S. news organizations, including
8 individuals or groups associated with known mercenary cyber threat actors.
9 On information and belief, the individuals and entities identified by the GRA
10 Defendants and used by the Qatari Defendants to attack Plaintiffs are:
11 Omniscope Limited, a U.K. security and intelligence firm; a naturalized
12 Israeli citizen with a history of criminal activity; a retired Moroccan diplomat;
13 and a London-based strategic intelligence firm with offices in the United
14 States.

15 8. On information and belief, the Agent Defendants all participated
16 in the strategic planning for and execution of the attacks.

17 9. On information and belief, Defendant Muzin's company
18 (Defendant Stonington) conspired with the other Defendants from within the
19 United States to organize and disseminate Plaintiffs' stolen emails to media
20 organizations. Significantly, Defendant Muzin exhibited inside knowledge of
21 the attacks on Plaintiffs, and disclosed foreknowledge of future attacks to at
22 least one other potential victim to warn him against taking public positions
23 adverse to the State of Qatar. On information and belief, Defendant Muzin's
24 company (Defendant Stonington) was among the vehicles used by the State of
25 Qatar to funnel funds to others involved in the attack.

1 10. Defendant Muzin has admitted his culpability. Because of
2 Muzin's status as its registered foreign agent, Muzin's admission also binds
3 Defendant the State of Qatar.

4 11. On March 5, 2018, Defendant Muzin told Joel Mowbray, a
5 business associate of Plaintiff Broidy and a critic of both the State of Qatar
6 and of Muzin, that there was "more stuff coming" from the *New York Times*.
7 Indeed, there was: the *New York Times* published stories based on Plaintiffs'
8 stolen emails on March 22 and 26, 2018. In that same meeting, Muzin
9 discussed meetings he had with his client the State of Qatar while serving as
10 its registered agent. Muzin told Mowbray: "**Broidy's name comes up in**
11 **Embassy meetings often**" and "I definitely identified him as somebody who,
12 was not, didn't like them too much." **Muzin further acknowledged that**
13 **everyone he "fingered" was "in danger."** He warned Mowbray that
14 Mowbray and Plaintiff Broidy needed "to be very careful," that **the State of**
15 **Qatar is "going after you,"** and that **"Honestly, I know they're after you**
16 **and Broidy."**

17 12. At that meeting, Muzin tried to persuade Mowbray that the
18 blame for the hacks on Plaintiffs and attempted hacks on Mowbray and
19 subsequent media leaks should fall on Muzin's principal (the State of Qatar)
20 and not Muzin because "I was doing my job." **Muzin was aware that the**
21 **State of Qatar utilized computer hacking as one of its cyber-weapons and**
22 **even admitted to Mowbray that he was "positive" that he himself had**
23 **been hacked by the Qataris.** Muzin's admissions to Mowbray inculcate
24 both Muzin and his principal and co-conspirator the State of Qatar, since
25 Muzin admitted that he and his principal orchestrated and participated in the
26 scheme to harm Plaintiffs by hacking and disseminating their computer
27 systems and information.

1 13. Somewhat belatedly, recognizing that he had admitted his
2 culpability and that of the State of Qatar to Mowbray, Muzin stated that he
3 realized that he needed “to be a little more careful” when he spoke to
4 Mowbray.

5 14. Defendants’ unlawful activity was directed toward the United
6 States and much of that activity occurred within the United States, including
7 the formation of the conspiracy in the United States during meetings in
8 Washington, D.C. The participants in these meetings were not engaged in
9 activities related to Qatar’s discretionary foreign policy, but instead were
10 conspiring to violate United States criminal and civil laws by targeting a
11 United States citizen for retribution because he had exercised his First
12 Amendment right to speak out publicly and privately to United States
13 government officials against the State of Qatar’s support for terrorist
14 organizations.

15 15. The hack, and the resulting unlawful access to Plaintiffs’ private
16 communications, documents, trade secrets and intellectual property, occurred
17 in the United States. Defendants conspired to design, coordinate and execute
18 an unlawful spearphishing campaign against several U.S. persons affiliated
19 with Plaintiff Broidy that included the following: spoofing or otherwise
20 obfuscating U.S.-assigned phone numbers to deceive several persons in the
21 United States into providing their email login credentials; misappropriating
22 the trademarks of U.S. companies such as Google LLC, a subsidiary of
23 Alphabet, Inc; fraudulently registering online website domains in the United
24 States; stealing email and online account login credentials for several U.S.
25 persons; illegally intruding into Plaintiffs’ email server in Los Angeles as well
26 as California servers of U.S.-based Google; stealing emails from those U.S.-
27 based servers; and then printing collections of Plaintiffs’ stolen electronic files

1 from within North America, sorting them by topic, and delivering them (in
2 some cases by hand) to news organizations in the United States, knowing that
3 the news organizations would publish the stolen emails under the cloak of the
4 First Amendment – all for the purpose of discrediting Plaintiff Broidy in the
5 United States and interfering with his business relationships. Defendants’
6 efforts to target Plaintiff Broidy in this manner have been largely successful:
7 several media organizations published articles (including front page stories in
8 the March 22 and 26, 2018 editions of the *New York Times*, a March 26, 2018
9 story by the Associated Press, a story in the March 1, 2018 edition of the *Wall*
10 *Street Journal*, and additional articles in *The Huffington Post*, *McClatchy*,
11 *Esquire*, *The Intercept* and *Bloomberg News*, which stories were reprinted or
12 summarized by numerous other news outlets). As recently as May 21, 2018,
13 the Associated Press published a story based on the hacked materials. In some
14 instances, these news organizations have acknowledged that those articles
15 were based on information they received from sources who boasted that the
16 materials were hacked from Plaintiffs’ computers.

17 16. As a result of Defendants’ actions, Plaintiffs, and in particular
18 Plaintiff Broidy, have been harmed, and will continue to be harmed.

19 PARTIES

20 17. Plaintiff Broidy Capital Management LLC is an investment firm
21 run by Plaintiff Elliott Broidy. BCM is a corporation duly organized under
22 the laws of the State of California with its principal place of business in Los
23 Angeles, California.

24 18. Plaintiff Elliott Broidy is a citizen of the United States and the
25 State of California who resides in Los Angeles, California. He is the Chief
26 Executive Officer and Chairman of BCM.

1 19. Defendant the State of Qatar is a foreign state. The head of state
2 and head of government of Qatar is the current Emir of Qatar, Sheikh Tamim
3 bin Hamad Al Thani. The Emir has made visits to Los Angeles, California
4 and has hosted the Mayor of Los Angeles, Eric Garcetti, in Doha, the capital
5 of Qatar, as part of an effort to strengthen the partnership between the cities of
6 Los Angeles and Doha. Additionally, the State of Qatar maintains a
7 Consulate in Los Angeles, California.

8 20. Defendant Stonington Strategies LLC is a public relations and
9 lobbying firm incorporated under the laws of Delaware. Upon information
10 and belief, Stonington's principal place of business is in New York, New
11 York. Stonington registered on September 3, 2017 under the Foreign Agents
12 Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, as a foreign agent
13 providing "strategic communications" for the State of Qatar. Stonington
14 originally was retained to provide these services for \$50,000 per month. On
15 November 1, 2017, shortly before the hacks on Plaintiff's computers began,
16 Defendant the State of Qatar increased the amount by a factor of six – to
17 \$300,000 per month.

18 21. Defendant Nicolas D. Muzin is the Chief Executive Officer of
19 Stonington and a political lobbyist who signed the FARA documents on
20 behalf of Stonington as a registered foreign agent of the State of Qatar. He is
21 a graduate of Yale Law School and a high-level Republican political
22 operative. Muzin served as chief of staff to then-Congressman (now Senator)
23 Tim Scott and served as deputy chief of staff for strategy to Senator Ted Cruz.
24 According to his biography on the Stonington website, Muzin also worked on
25 the Trump Presidential campaign as well as on the transition team to recruit
26 candidates for the new Administration. Shortly after the inauguration of
27 President Donald J. Trump, Muzin began working as a lobbyist, first

1 registering as a FARA agent for the Democratic Party of Albania in March
2 2017. On August 24, 2017, he was retained by the State of Qatar for
3 “consulting services.” More recently, on May 14, 2018, Muzin was
4 photographed at the opening of the United States Embassy in Jerusalem with
5 Senator Cruz and White House aide Victoria Coates, the Senior Director for
6 International Negotiations on the National Security Council and a former aide
7 to Senator Cruz. Defendant Muzin is a citizen of the United States and a
8 resident of the state of Maryland. On information and belief, Muzin has
9 frequently traveled to California for business and political purposes during
10 recent years.

11 22. Defendant Global Risk Advisors, LLC is a limited liability
12 company formed under the laws of Delaware, with its primary place of
13 business in New York, New York. It has not registered as a FARA agent of
14 the State of Qatar.

15 23. Defendant Kevin Chalker is the founder and Chief Executive
16 Officer of GRA. Upon information and belief, he is a citizen of the United
17 States and is domiciled in the state of New York. Chalker has not registered
18 as a FARA agent of the State of Qatar.

19 24. Defendant David Mark Powell is a Managing Director of GRA
20 and also is the Principal Agent of GRA in Qatar. On information and belief,
21 Powell is a citizen of the United Kingdom and is domiciled in the United
22 Kingdom.

23 25. On October 26, 2017, only a few weeks before Defendants began
24 their efforts to unlawfully access Plaintiffs’ emails, documents, trade secrets
25 and intellectual property, GRA, acting through a wholly-owned subsidiary –
26 Global Risk Advisors (EMEA) Limited, a Gibraltar corporation, headed by
27 Defendant David Mark Powell – began to operate in Qatar.

1 26. Defendant Mohammed bin Hamad bin Khalifa Al Thani, who
2 received his degrees from Georgetown and Harvard, is a brother of the Emir
3 of Qatar. According to articles in *Sports Illustrated* on May 23, 2011 and *The*
4 *Telegraph* on March 18, 2014, Defendant Al Thani has been accused of
5 bribery and human rights abuses in connection with Qatar's successful bid to
6 host the 2022 FIFA World Cup and the subsequent construction of the
7 necessary facilities, which *The Guardian* reported on September 25, 2013
8 resulted in the "exploitation and abuses" of Nepalese workers "that amount to
9 modern-day slavery."

10 27. On information and belief, after its neighboring Middle Eastern
11 countries began their quarantine of Qatar in 2017, Defendant the State of
12 Qatar charged Defendant Al Thani with the task of attempting to influence
13 United States public opinion, and the position of the Trump Administration.
14 For example, as reported in *Politico* on May 8, 2018, the State of Qatar's
15 ongoing efforts to purchase Newsmax, a conservative news outlet with ties to
16 the Trump Administration, were "overseen by Mohammed bin Hamad bin
17 Khalifa Al Thani, a younger brother of Qatari Emir Tamim bin Hamad Al
18 Thani" and "came during a mad scramble by the wealthy Gulf monarchy to
19 win friends and clout in the United States as it struggled to respond to a
20 Trump-endorsed blockade by its Arab neighbors." On information and belief,
21 Al Thani also specifically directed the effort to address impediments to the
22 success of Qatar's program to influence United States public opinion and the
23 position of the Trump Administration on the embargo, including specifically
24 the efforts to attack and discredit Plaintiff Broidy.

25 28. Defendant Ahmed Al-Rumaihi is a citizen of the State of Qatar
26 and a former Qatari diplomat. In the time period beginning in April 2017 and
27 continuing to the present, Defendant Al-Rumaihi has not held an official

1 position in the Government of the State of Qatar (according to the State of
2 Qatar), but on information and belief has continued to act as an agent of the
3 State of Qatar. Al-Rumaihi is a resident of Qatar.

4 29. On information and belief, Defendants Does 1-10 are agents of
5 the State of Qatar, some of whom have not registered under FARA. On
6 information and belief, none of Defendants Does 1-10 is a citizen or resident
7 of the State of California.

8 **JURISDICTION AND VENUE**

9 **I. SUBJECT MATTER JURISDICTION**

10 30. This Court has subject matter jurisdiction over the State of Qatar
11 pursuant to 28 U.S.C. § 1330 and the Foreign Sovereign Immunities Act, 28
12 U.S.C. § 1602 *et seq.*, because its conduct falls within the exception to foreign
13 sovereign immunity set forth in 28 U.S.C. § 1605(a)(5). Multiple entire torts
14 as described herein occurred within the United States, and additional tortious
15 misconduct described herein occurred at a minimum predominately within the
16 United States.

17 31. This Court also has subject matter jurisdiction over the State of
18 Qatar because its conduct falls within the exception to foreign sovereign
19 immunity set forth in 28 U.S.C. § 1605(a)(2). The State of Qatar entered into
20 numerous commercial contracts with persons to provide consulting, public
21 relations, offensive cyber and other lawful and unlawful commercial services
22 in order to further the State of Qatar's public relations efforts and economic
23 and commercial interests, which included most significantly the lifting of a
24 comprehensive trade and commercial embargo on Qatar. In furtherance of
25 those commercial contracts, Defendants then targeted Plaintiff Broidy. Upon
26 information and belief, the State of Qatar engaged the GRA Defendants and
27 the Agent Defendants to use illegal commercial means to promote its own

1 economic and commercial interests, including by conducting economic
2 espionage. These forms of commercial activity directly affected the United
3 States.

4 32. This Court further has subject matter jurisdiction over this action
5 under 28 U.S.C. § 1331, and supplemental jurisdiction over Plaintiffs' state
6 law claims under 28 U.S.C. § 1367. Additionally, this Court has subject
7 matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332 because
8 Plaintiffs are all citizens of the state of California and, to Plaintiffs'
9 knowledge, none of the Defendants is a citizen of the State of California.
10 Accordingly, the citizenship of the parties is diverse. The amount in
11 controversy exceeds \$75,000, exclusive of interest and costs.

12 **II. PERSONAL JURISDICTION**

13 33. This Court has personal jurisdiction over the State of Qatar
14 pursuant to 28 U.S.C. § 1330 and the Foreign Sovereign Immunities Act, 28
15 U.S.C. § 1602 *et seq.*, because its conduct falls within the exception to foreign
16 sovereign immunity set forth in 28 U.S.C. § 1605(a)(5) and § 1605(a)(2).

17 34. Plaintiffs served the State of Qatar pursuant to 28 U.S.C.
18 § 1608(a).

19 35. This Court has personal jurisdiction over the Agent Defendants
20 and the Qatari Defendants other than the State of Qatar itself under the state of
21 California's long-arm statute, Cal. Civ. Proc. Code § 410.10, because they
22 directly or as a result of their participation in the conspiracy described herein,
23 targeted Plaintiffs in California and directed their tortious conduct towards
24 Plaintiffs in California, with knowledge and intent that Plaintiffs suffer harm
25 in California.

1 36. On information and belief, Defendant Al-Rumaihi leases
2 property in California, conducts substantial business in California, and has
3 sufficient and substantial contacts with this jurisdiction.

4 **III. VENUE**

5 37. Venue is proper in this judicial district under 28 U.S.C.
6 § 1391(b)(2) because a substantial part of the events or omissions giving rise
7 to this claim occurred in this judicial district, and a substantial part of property
8 that is the subject of this action is situated in this judicial district. In
9 particular, the private communications, documents, trade secrets and
10 intellectual property that was unlawfully accessed, converted, and stolen was
11 located in this district and the unlawful access to those materials necessarily
12 took place in this district.

13 38. Venue also is proper in this judicial district under 28 U.S.C.
14 §1391(f)(1) for the same reasons and because Defendant the State of Qatar is
15 a foreign state.

16 39. Alternatively, venue is proper in this judicial district under 28
17 U.S.C. § 1391(b)(3) because there is no judicial district in a State in which all
18 non-foreign defendants are resident, and at least one Defendant is subject to
19 personal jurisdiction in California.

20 **STATEMENT OF FACTS**

21 40. This is a case about a civil and criminal conspiracy undertaken by
22 a foreign nation on the territory of the United States against a successful,
23 influential United States citizen and his California corporation. Qatar targeted
24 Plaintiff Broidy because he spoke out forcefully and effectively against
25 Qatar's support for terrorism, entered into significant business relationships
26 relating to defense and counterterrorism with a neighboring nation, and stood
27

1 in the way of relieving commercial pressures resulting from a devastating
2 economic embargo. The purpose of the conspiracy targeting Broidy was to
3 use illegal means to diminish his influence within the United States through a
4 campaign to discredit him in the press and in the eyes of U.S. government
5 officials, and to disrupt Plaintiffs' business relationships. The conspiracy
6 included the commissioned hacking of Plaintiffs' computer networks, which
7 were located in the United States during the relevant timeframe, including
8 Plaintiffs' email accounts, and transmission of the illicitly obtained data to the
9 media.

10 **I. INTERNATIONAL SANCTIONS WERE IMPOSED ON THE**
11 **STATE OF QATAR IN JUNE 2017 AS THE RESULT OF ITS**
12 **HISTORY OF SUPPORTING AND HARBORING TERRORISTS**

12 41. Defendant the State of Qatar sponsors and supports terrorists,
13 having once been called a "Club Med for Terrorists." Qatar has allowed and
14 continues to allow itself to serve as a sanctuary for terrorist leaders and
15 organizations, including but not limited to Al Qaeda (and its affiliates
16 including Al-Shabab and Al Qaeda in Syria, also known as Al-Nusra Front or
17 Jabhat Al-Nusra), Hamas, the Taliban, and the Muslim Brotherhood.

18 42. Numerous individuals residing in Qatar have been sanctioned by
19 the United States Department of Treasury for raising funds for Al Qaeda.

20 43. Individuals who serve as fundraisers for Al Qaeda's Syrian
21 franchise (the Nusra Front) operate freely in Qatar. These individuals appear
22 at state-owned Mosques and on broadcasts aired by the state-funded Al
23 Jazeera. The State of Qatar has failed to shut down these fundraisers.

24 44. The State of Qatar also has been accused of hosting the Somali
25 terrorist group Al-Shabab, an Al Qaeda affiliate.

26 45. The State of Qatar also has permitted Hamas leaders to operate
27 freely within the country. Indeed, the State of Qatar has provided substantial

1 funding to Hamas, despite being subjected to international political and
2 economic sanctions for such support.

3 46. The State of Qatar has further allowed the Taliban to operate and
4 maintain an office in Doha.

5 47. The State of Qatar has given safe haven to many leaders of the
6 Muslim Brotherhood after their expulsion from Egypt by the Egyptian
7 government.

8 48. On May 25, 2017, a bill (H.R. 2712) was introduced in the
9 United States House of Representatives titled “The Palestinian International
10 Terrorism Support Prevention Act of 2017.” The bill, which would have
11 barred assistance from the United States government to any country that aided
12 Hamas, stated in its findings that “Hamas has received significant financial
13 and military support from Qatar.”

14 49. On June 5, 2017, neighboring Middle Eastern states severed
15 diplomatic relations with the State of Qatar because of the State of Qatar’s
16 support for terrorism and its close ties to Iran. Other governments quickly
17 followed. Some countries closed their airspaces to Qatari aircraft, closed their
18 borders with the State of Qatar and/or banned Qatari-flagged ships from
19 docking at their ports. The sanctioning states issued a set of demands to the
20 State of Qatar including that the State of Qatar curb ties with Iran and stop
21 funding terrorist organizations. Those demands were rejected.

22 50. President Trump denounced Qatar and sided with the efforts to
23 embargo Qatar, tweeting on June 6, 2017: “During my recent trip to the
24 Middle East I stated that there can no longer be funding of Radical Ideology.
25 Leaders pointed to Qatar - look!”

1 51. On June 9, 2017, once again siding with the sanctioning states
2 and criticizing the more conciliatory tone of the then-Secretary of State,
3 President Trump stated:

4 The nation of Qatar, unfortunately, has historically been a funder
5 of terrorism at a very high level, and... nations came together and
6 spoke to me about confronting Qatar over its behavior. So we
7 had a decision to make: Do we take the easy road, or do we
8 finally take a hard but necessary action? We have to stop the
9 funding of terrorism. I decided, along with Secretary of State
10 Rex Tillerson, our great generals and military people, the time
11 had come to call on Qatar to end its funding — they have to end
12 that funding — and its extremist ideology in terms of funding...
13 This is my great priority because it is my first duty as President to
14 keep our people safe. Defeating ISIS and other terror
15 organizations is something I have emphasized all during my
16 campaign and right up until the present. To do that, stop funding,
17 stop teaching hate, and stop the killing. For Qatar, we want you
18 back among the unity of responsible nations.

12 52. Defendant State of Qatar is a nation rich in natural gas resources,
13 but it is reliant on food and other supplies that arrive by truck via borders that
14 closed as part of the embargo. The international sanctions – and the support
15 the President Trump expressed for them – threatened to damage Qatar’s
16 economy and plunged Qatar into crisis. The sanctioning states threatened to
17 expel the State of Qatar from the Gulf Cooperation Council, a regional
18 economic and security cooperation body made up of six nations. The
19 economic quarantine led to a massive drop-off in foreign investment in Qatar.
20 According to the International Monetary Fund, “following the rift, foreign
21 financing (non-resident deposits and inter-bank placements) and resident
22 private-sector deposits fell by about US\$40 billion.”

23 53. These international sanctions on the State of Qatar remain in
24 effect today.

1 **II. THE STATE OF QATAR BEGAN A PUBLIC RELATIONS**
2 **CAMPAIGN TO IMPROVE ITS IMAGE IN THE UNITED**
3 **STATES, WHICH HAS SUPPORTED THE INTERNATIONAL**
4 **SANCTIONS AGAINST QATAR**

5 54. As a result of its Middle Eastern neighbors severing diplomatic
6 relations and imposing a commercial blockade, the Qatari Defendants retained
7 agents in Washington, D.C. and paid them millions of dollars to impact public
8 opinion and public policy in the United States, including by entering into
9 specific agreements with those agents for those agents to provide public
10 relations, consultancy, and related services. The Qatari Defendants launched
11 a public relations campaign to obfuscate Qatar's ties to, and financial and
12 logistical support of, some of the world's worst extremist and terrorist
13 organizations—including Al Qaeda (and its affiliate Al-Shabab), Hamas, the
14 Taliban, and the Muslim Brotherhood—and to change Qatar's image in the
15 United States, including particularly in the Jewish community in the United
16 States. As *Tablet Magazine*, an online publication focused on Jewish news,
17 wrote on February 13, 2018, the Qatari influence operation reflected “a Qatari
18 preoccupation with American Jewish communal power, as well as a desire to
19 address whichever challenges Doha believes Jewish influence raises for the
20 country's vast ambitions in Washington and beyond.”

21 55. This campaign was aimed at: (1) bolstering the image of the State
22 of Qatar in circles perceived as influential with the Trump Administration;
23 and (2) curtailing the influence of individuals that could undermine the
24 standing of the State of Qatar in the United States.
25
26
27
28

A. Al Thani and Al-Rumaihi Directed and Supervised The State Of Qatar's Whitewashing Efforts

56. This campaign on behalf of Defendant the State of Qatar was directed and supervised by its agents Defendant Al Thani and Defendant Al-Rumaihi.

57. One of the activities engaged in by Defendant Al-Rumaihi was investing in entities that he and Defendant Al Thani thought could help to bolster Qatar's image in the United States. Al-Rumaihi and Al Thani have access to billions of dollars in capital from the Qatar Investment Authority to use for this purpose. As one example, in 2017 Al-Rumaihi was a significant investor in the "Big3" basketball league, started by Rapper Ice Cube and Jeff Kwatinetz, a Los Angeles businessman. Al-Rumaihi then sought to use his association with Kwatinetz to gain contact with Kwatinetz's former business associate, Steve Bannon, who was at that time the Chief White House Strategist for President Trump. In litigation relating to Al-Rumaihi's investment in Big3, Kwatinetz filed an affidavit stating: "there were numerous occasions during the 2017 [Big3] season, where Mr. Al-Rumaihi would bring up Mr. Bannon's name to me and comment about Mr. Bannon's political positions, his views on the blockade [of Qatar by Gulf states], the Trump administration's position toward Qatar, and he persistently inquired about wanting to meet with Mr. Bannon."

58. In an affidavit filed in that litigation, Kwatinetz further revealed that Defendant Al-Rumaihi admitted that he had previously attempted to financially influence former officials of the Trump Administration:

Mr. Al-Rumaihi stated to me [Kwatinetz] that he wanted me to convey a message from the Qatari Government to Steve Bannon. Mr. Al-Rumaihi requested I set up a meeting between him, the Qatari government, and Steven Bannon, and to tell Steve Bannon that Qatar would underwrite all of his political efforts in return for his support. I immediately let Mr. Al-Rumaihi know that I

1 was offended by this request, that I was trying to run a basketball
2 league and need our money paid, and I stated that neither I nor
3 Steve Bannon would ever take, or even entertain the concept, of a
4 bribe of any kind. I was appalled. Mr. Al-Rumaihi laughed and
5 then stated to me that I shouldn't be naive, that so many
6 Washington politicians take our money, and stated "do you think
7 [former National Security Advisor Michael] Flynn turned down
8 our money?"

9
10 59. On information and belief, Defendant Al-Rumaihi's comments to
11 Kwatinetz reference a December 12, 2016 visit by Al-Rumaihi to Trump
12 Tower to visit with the Trump Transition Team. Michael Flynn, at that time
13 the incoming National Security Adviser, was at Trump Tower on that same
14 day. Both Al-Rumaihi and Flynn were photographed in the lobby of the
15 Trump Tower that day.

16 60. The attempted purchase of *Newsmax* is another example of how
17 Al-Rumaihi and Al Thani sought to use millions of dollars from the Qatari
18 Investment Authority to bolster Qatar's image in the United States in an effort
19 to address the commercial embargo. *Politico* reported on May 8, 2018 that
20 the State of Qatar's attempt to purchase *Newsmax* was "overseen by
21 Mohammed bin Hamad bin Khalifa Al Thani, a younger brother of Qatari
22 Emir Tamim bin Hamad Al Thani" and "came during a mad scramble by the
23 wealthy Gulf monarchy to win friends and clout in the United States as it
24 struggled to respond to a Trump-endorsed blockade by its Arab neighbors."

25 61. Defendant Al-Rumaihi retained additional agents to craft and
26 execute the State of Qatar's image whitewashing campaign. For example, Al-
27 Rumaihi was identified as the contact for Qatar in the June 7, 2017 retainer
28 agreement between the Ashcroft Law Firm LLC and the "Government of
Qatar." According to the FARA filing disclosing that contract, former
Attorney General Ashcroft was retained by the Qatari Defendants to "enlist
the support and expertise of former key government leaders, including former

1 officials who held very senior positions within the Intelligence Community,
2 the Federal Bureau of Investigation, the Department of Treasury and the
3 Department of Homeland Security[.]” That \$2.5 million retainer agreement
4 was signed for the State of Qatar by Dr. Ahmed Al-Hammadi, the Secretary
5 General of the State of Qatar’s Ministry of Foreign Affairs and the Acting
6 Head of Investments of the State-owned Qatar Investment Authority.

7 **B. Defendants Stonington And Muzin Initially Focused On**
8 **Influencing The United States Jewish Community**

9 62. Upon information and belief, as described in the February 13,
10 2018 *Tablet Magazine* article, Defendant Al-Rumaihi worked with
11 unregistered Qatari agent Joey Allaham to identify Defendants Muzin and
12 Stonington to assist in the State of Qatar’s campaign to influence the Jewish
13 community in the United States.

14 63. In late August 2017, the Qatari Defendants retained Defendants
15 Stonington and Muzin to influence public opinion regarding the State of
16 Qatar. Their agreement specifies that Muzin and Stonington were to provide
17 “consulting services” including the “development and implementation of a
18 government relations strategy for the State of Qatar, as requested and directed
19 by the Embassy.” The initial agreement provided that the State of Qatar
20 would pay Muzin and Stonington \$50,000 a month for these services.

21 64. Defendant Muzin’s efforts as an agent of the State of Qatar
22 quickly focused on an effort to put a pro-Jewish spin on the State of Qatar. A
23 September 5, 2017 article in *O’Dwyer’s*, an online magazine covering the
24 public relations industry, quotes Muzin as stating: “Engagement with Qatar
25 can only be in the best interests of the United States and the Jewish
26 community, as we cannot allow Qatar to be ostracized by its neighbors and
27 pushed into Iran’s sphere of influence.”

65. As reported by the Israeli newspaper *Haaretz* on September 28, 2017, Defendant Muzin invited American Jewish leaders to meet with the Emir in New York City during the Emir's visit for the United Nations General Assembly later that month. The opposition of Plaintiff Broidy and others to these efforts helped prompt American Jewish leaders to refuse to meet with the Emir at that gathering, thereby frustrating the plans of the Qatari Defendants and Defendants Muzin, and Stonington to win over Jewish leaders.

66. The Zionist Organization of America ("ZOA") reacted to that invitation with a press release on September 12, 2017, in which the organization's president, Morton A. Klein, stated that although he had "received an invitation to meet with" the Emir of Qatar during the United Nations General Assembly, he had "decided not to accept this invitation." Mr. Klein further stated: "Any Jewish leader meeting with the Qatari Emir or Crown Prince likely means well, but he will serve as an unwitting prop in their PR ploy to whitewash the legitimate reasons why its Arab Muslim neighbors are boycotting them and why Israel and Jews are horrified by them, meaning it will only strengthen Qatar's embrace of Iran and critical backing of Hamas."

67. According to a February 13, 2018 article in *Tablet Magazine*, "Muzin largely failed to persuade Jewish leaders to agree to meetings with influential Qataris visiting New York for the opening of the United Nations General Assembly."

68. Soon after the failure of the United Nations General Assembly initiative, Muzin began to invite American Jewish leaders on all-expense-paid trips to Qatar to further the State of Qatar's public relations campaign. Plaintiff Broidy and others again encouraged American Jewish leaders to

1 decline the invitations. These efforts were mostly successful in helping to
2 prompt many American Jewish leaders to decline to participate in the public
3 relations trips to Qatar.

4 69. As part of his work for the State of Qatar, Muzin sought out high-
5 profile individuals who could be helpful in furthering the interests of the State
6 of Qatar. On information and belief, Defendant Muzin recruited former
7 Arkansas Governor Mike Huckabee, a Republican candidate for President,
8 prominent media commentator, and father of current White House Press
9 Secretary Sarah Huckabee Sanders, to participate on a trip to Qatar. On
10 January 8, 2018, former Governor Huckabee tweeted “I’m in Doha,” and then
11 on January 12, 2018, tweeted, “Just back from a few days in surprisingly
12 beautiful, modern, and hospitable Doha[.]” On information and belief
13 Defendant Muzin acknowledged paying an individual \$50,000 for doing work
14 related to influencing former Governor Huckabee to travel to Qatar and meet
15 with the Emir.

16 70. On information and belief, Defendant Muzin also met with White
17 House aide Victoria Coates, the Senior Director for International Negotiations
18 on the National Security Council and a former aide to Senator Ted Cruz, to
19 advocate for United States policies that would be supportive of the State of
20 Qatar. On information and belief, Defendant Muzin got Coates to have her
21 boss, Jason Greenblatt, the Special Envoy for International Negotiations, send
22 out the following tweet on February 9, 2018, that was supportive of Qatar:
23 “Qatar partnering with Israel can bring real relief to the people of Gaza.
24 Ending support for Hamas and focusing on humanitarian aid and
25 reconstruction will end the suffering.”

26 71. Defendant Al-Rumaihi also engaged in efforts similar to
27 Defendants Muzin and Stonington with respect to the United States Jewish

1 Community. By means of example, at the invitation of unregistered Qatari
2 agent Joey Allaham, Al-Rumaihi attended a gala for the ZOA in New York
3 City in November 2017. Despite having vocally rejected an invitation by
4 Defendant Muzin to meet with the Emir at the United Nations General
5 Assembly in September 2017, after this dinner, the President of the ZOA
6 (Morton A. Klein) visited Qatar on a trip that Muzin arranged.

7 **C. The State Of Qatar Spent Millions of Dollars on Agents To**
8 **Further Its Public And Governmental Relations Efforts in the**
9 **United States**

10 72. According to the Center for Responsive Politics, the State of
11 Qatar spent nearly five million dollars on lobbyists and media relations in
12 2017 in an effort to gain the support of the United States government in
13 Qatar's its diplomatic standoff with other Middle Eastern countries.

14 73. According to FARA filings of the State of Qatar, it retained and
15 entered into written agreements with at least the following agents in the
16 second half of 2017 or the first quarter of 2018 in an effort to improve its
17 image in the United States.

- 18 a. Avenue Strategies Global LLC (July 17, 2017 agreement), a
19 firm with which former Trump Campaign Manager Corey
20 Lewandowski has been affiliated, at the rate of \$150,000 per
21 month, increased to \$500,000 per month on September 5,
22 2017, with an additional \$250,000 added to the October
23 invoice through a retroactive agreement dated February 28,
24 2018;

- b. Stonington Strategies LLC (August 24, 2017 agreement) at the rate of \$50,000 per month, increased to \$300,000 per month on November 1, 2017;²
- c. Ashcroft Law Group (June 7, 2017 agreement), at the rate of \$2.5 million for a 90-day retainer;
- d. Levick Strategic Communications (June 5, 2017 agreement) at the rate of \$54,000 per month;
- e. Information Management Services Inc. (June 19, 2017 agreement) at the rate of \$375,000 per month;
- f. Conover & Gould Strategic Communications (June 29, 2017 agreement) at the rate of \$100,000 per month;
- g. Gallagher Group (July 11, 2017 agreement) at the rate of \$25,000 per month, amended February 5, 2018 to \$45,000 per month;
- h. Audience Partners Worldwide (July 28, 2017 agreement) at an undisclosed rate;
- i. McDermott, Will & Emery (July 13, 2017 agreement) at the rate of \$40,000 per month;
- j. Nelson Mullins Riley & Scarborough LLP (July 26, 2017 agreement, renewed on March 19, 2018) at the rate of \$100,000 per month for three months;
- k. Portland PR (December 6, 2017 agreement) at the rate of \$123,195 per month;

² Stonington notably has not filed its mandatory supplemental FARA filing disclosing the specifics of its FARA activities. That filing was due in March 2018. 28 C.F.R. § 5.200.

- 1 l. Mercury Public Affairs (September 7, 2017 agreement) at the
- 2 rate of \$120,000 per month;
- 3 m. Bluefront Strategies (September 12, 2017 agreement)
- 4 \$100,000;
- 5 n. Hawksbill Group (August 1, 2017 agreement) \$165,000;
- 6 o. Vitello Consulting (December 6, 2017 agreement) \$10,000, as
- 7 a subcontractor of Stonington Strategies;
- 8 p. Iron Bridge Strategies (February 1, 2018 agreement) at the
- 9 rate of \$25,000 per month;
- 10 q. Tigercomm LLC (January 11, 2018 agreement) at the rate of
- 11 \$30,000 per month;
- 12 r. Venable LLP (January 31, 2018 agreement) at the rate of
- 13 \$150,000 per month;
- 14 s. Husch Blackwell Strategies (February 1, 2018 agreement) at
- 15 the rate of \$25,000 per month;
- 16 t. SGR Government Relations & Lobbying (February 1, 2018
- 17 agreement) at the rate of \$40,000 per month;
- 18 u. Pillsbury Winthrop Shaw Pittman LLP (March 15, 2018
- 19 agreement) at rates between \$500 and \$955 per hour;
- 20 v. Lumen8 Advisors, LLC (March 15, 2018 agreement) at the
- 21 rate of \$1,000 per hour; and
- 22 w. Ballard Partners (March 29, 2018 Agreement) at the rate of
- 23 \$175,000 per month for one year.

24 **III. DEFENDANTS BECAME INCREASINGLY FRUSTRATED BY**

25 **PLAINTIFF BROIDY'S OUTSPOKEN CRITICISM OF THE**

26 **STATE OF QATAR**

27 74. Plaintiff Broidy is a prominent business and civic leader who has

28 actively served in leadership roles in Jewish organizations and the Republican

1 Party for decades, and during pertinent periods frequently and directly
2 interacted with the President of the United States. His advocacy against
3 terrorism and extremism is well known. Plaintiff Broidy served on the
4 Homeland Security Advisory Council from 2006 to 2009 and specifically on
5 the Future of Terrorism Task Force of that Council. The “Findings” report of
6 that Task Force, issued on January 11, 2007, stated: “Factors that will
7 influence the future of terrorism include: the leadership of the terrorists, US
8 counterterrorism efforts, status of political reform in Muslim nations and *the*
9 *elimination of safe havens[.]*” (Emphasis added.) This report was directed at
10 and, on information and belief, was known to countries operating as safe
11 havens for terrorist organizations, including the State of Qatar.

12 75. Since September 11, 2001, Plaintiff Broidy has increased his
13 involvement in supporting the safety of his homeland, the United States. As
14 part of his involvement, he became active in fundraising for the Republican
15 Party because its views on how to defend the United States were aligned with
16 his own. He also became involved in numerous civic activities involving
17 counter-terrorism to promote the security of the United States.

18 76. Beginning in March 2017, Plaintiff Broidy, among others,
19 became a vocal critic of the State of Qatar’s support for terrorists and friendly
20 relationship with Iran, which Mr. Broidy sees as a major threat to the security
21 of the United States and its allies, and began to support financially public
22 initiatives – such as conferences – to educate Americans about Qatar’s support
23 for terrorist and extremist organizations.

24 77. During pertinent periods Plaintiff Broidy regularly conveyed this
25 criticism of Qatar in meetings with United States Government officials and
26 civic leaders, including President Trump.

1 78. Defendant the State of Qatar was aware of Plaintiff Broidy's
2 influential criticism. In initial discussions with Defendants Muzin and
3 Stonington, Qatari officials told Muzin of their concerns about Plaintiff
4 Broidy. As Defendant Muzin recounted, "They knew about him [Broidy]"
5 and "knew that he [Broidy] had been influential" in shaping the White
6 House's views on Qatar.

7 79. Qatari officials complained in particular about President Trump's
8 recorded remarks at a June 2017 meeting of the Republican National
9 Committee: "We're having a dispute with Qatar — we're supposed to say
10 Qatar. It's Qatar, they prefer. I prefer that they don't fund terrorism." At
11 the same meeting, President Trump publicly identified Plaintiff Broidy in the
12 audience and stated: "Elliott Broidy is fantastic." That acknowledgment was
13 followed by a round of applause.

14 80. Defendant Muzin has admitted that officials of Defendant the
15 State of Qatar, with whom he met shortly after President Trump's remarks
16 at that June 2017 meeting, stated: "Broidy was like sitting in the front row
17 and that he had somehow prompted Trump to say that."

18 81. After Defendants Muzin and Stonington were retained by the
19 State of Qatar, Mr. Broidy extended his criticism of the State of Qatar to the
20 efforts by Muzin and Stonington to arrange meetings between the Emir and
21 American Jewish leaders.

22 82. Beginning in or around September 2017, Plaintiff Broidy began
23 to urge American Jewish leaders to decline the invitations of the State of
24 Qatar and Muzin to meet with the Emir in New York City and/or to visit
25 Qatar.

26 83. Plaintiff Broidy was not alone in this effort. On September 15,
27 2017, *Forbes* published a piece by a contributing writer titled "Why is Qatar

1 offering to trade dead Israelis for meetings with live Jews?” The article
2 reported that an offer was being made to American Jewish leaders to return
3 the corpses of two Israeli soldiers whom Hamas had killed if those leaders
4 would meet with the Emir. The article stated:

- 5 a. Rabbi Shmuel Boteach (who according to *Newsweek* is one of
6 the ten most influential rabbis in the United States) stated that
7 “all who agreed to whitewash the terror-stained hands of the
8 emir would be condoning murder.”
- 9 b. The State of Qatar hired Defendant Muzin, who “may have
10 hinted to some Jewish leaders that his lobbying had the
11 ‘blessing’ of Israel’s elected government.” But Israel’s
12 Ambassador to the United States, Ron Dermer, denied this,
13 stating: “It is not true.”
- 14 c. The State of Qatar has admitted to giving approximately \$1.4
15 billion to Hamas over the past few years. (Hamas is
16 designated by the United States as a terrorist organization).
- 17 d. Qatar is “like Woodstock for terrorists,” and has also “been
18 accused of hosting the Somali terrorist group Al-Shabab, an al
19 Qaeda affiliate.”
- 20 e. Defendant Muzin claimed that he contacted prominent
21 American Jewish leaders, but “Each denied agreeing to any
22 meeting with Qatar and two of these leaders denied ever even
23 speaking to Muzin.” “Like a child’s game of telephone,
24 Muzin apparently told each Jewish leader that a different
25 prominent Jew had already agreed to meet the Emir. This
26 didn’t turn out to be true.”

1 84. Although many American Jewish leaders declined the invitations
2 given in September 2017, Defendant Muzin continued his attempts to arrange
3 trips to Qatar for American Jewish leaders. These trips furthered the State of
4 Qatar's strategy to court favor with high-profile American Jewish leaders,
5 whom they believed could shift United States policy in favor of the State of
6 Qatar and alleviate pressure caused by the economic embargo on it. On
7 information and belief, in some instances, Defendants Muzin and Stonington
8 paid for the trips taken. Among those participating in the trips were:

- 9 a. Rabbi Shmully Hecht, co-founder and Rabbinical Advisor of
10 Shabtai, the Jewish Society at Yale University, who wrote in a
11 January 25, 2018 article in *The Times of Israel*, an online
12 Israeli newspaper: "A few months ago, Nick Muzin asked me
13 to attend meetings with influential global thought leaders who
14 are also prominent in the Jewish world, and the Emir of Qatar.
15 . . . Many prominent Jewish leaders have flown to Qatar and
16 have spent quality time with the country's leadership."
17 b. Alan Dershowitz, the Felix Frankfurter Professor of Law,
18 Emeritus, at Harvard Law School, who wrote in a January 12,
19 2018 article in *The Hill*: "I just returned from a private visit
20 to Qatar, at the invitation of and paid for by the Emir. . . . I
21 observed that Qatar is quickly becoming the Israel of the Gulf
22 States, surrounded by enemies, subject to boycotts and
23 unrealistic demands, and struggling for its survival."
24 Defendant Muzin acknowledged arranging for Dershowitz to
25 make this trip.
26 c. Morton A. Klein, the President of ZOA, who, despite his
27 initial reluctance to meet with the Emir at the United Nations,
28

1 ultimately decided to travel to Qatar in order to have the
2 chance to confront the Emir, wrote in a January 30, 2018
3 article in *Haaretz*: “I decided it was important for me to
4 speak truth to power, especially when the Emir repeatedly
5 invited me to give them my views on what they needed to
6 do.”

- 7 d. Malcolm Hoenlein, the executive vice chairman of the
8 Conference of Presidents of Major Jewish Organizations.
9 (During approximately the same time period in 2017,
10 Defendant Al Thani attended the wedding of Hoenlein’s
11 daughter).

12 85. Despite these successes, there was nonetheless significant
13 backlash in the American Jewish community against Defendant Muzin’s work
14 on behalf of the State of Qatar. For example:

- 15 a. On January 15, 2018, Rabbi Shmuel Boteach published “An
16 Open Letter to the Emir of Qatar,” stating: “Newspapers are
17 filled with reports that you have hired an Orthodox Jew, Nick
18 Muzin, of Stonington Strategies, and his partners, as agents of
19 Qatar to promote your image among American Jews, and to
20 lobby the US government. There is non-stop chatter of rabbis,
21 writers and community leaders accepting free trips to Doha,
22 which is big news because your regime funds Hamas —
23 which is responsible for an endless stream of funerals in
24 Israel.”
- 25 b. A spokesman for the Israeli Embassy in Washington
26 denounced the trips to Qatar. *See Haaretz* on January 31,
27 2018 (“We oppose this outreach effort in the Jewish and pro-

1 Israel community.”) and the *New York Times* on February 9,
2 2018 (“We do not approve of these visits by the Jewish
3 organizations to Qatar.”).

4 86. Plaintiff Broidy did not make any public statements against the
5 trips to Qatar, but he and others did privately criticize them with other
6 American Jewish leaders. Plaintiff Broidy also funded at least two high-
7 profile conferences in Washington, D.C. devoted to scrutiny of the State of
8 Qatar.

9 87. On information and belief, Plaintiff Broidy’s efforts opposing the
10 State of Qatar, and in particular the efforts of Muzin and Stonington on
11 Qatar’s behalf, only enhanced Muzin’s pre-existing animus against Broidy,
12 which arose from Broidy’s successful efforts in 2016 to block Muzin from
13 receiving a highly questionable commission on a large political donation that
14 Muzin believed he had been instrumental in arranging.

15 **IV. DEFENDANTS TARGET BROIDY**

16 88. In connection with his work for the State of Qatar, Defendant
17 Muzin had weekly meetings at the Embassy of Qatar in Washington, D.C.,
18 where he discussed his ongoing efforts. On information and belief, the
19 agendas for these meetings were set by Defendants Al Thani and Al-Rumaihi,
20 and the meetings began in 2017 in anticipation of the Emir’s April 2018 visit
21 to the United States for bilateral meetings with the Trump Administration and
22 visits to Capitol Hill. On information and belief, at those meetings, Defendant
23 Muzin became increasingly upset about Plaintiff Broidy’s efforts to
24 undermine his lobbying for the State of Qatar and felt that these were personal
25 attacks on him. On information and belief, Defendant Muzin brought up
26

1 Plaintiff Broidy in these meetings as an obstacle that needed to be dealt with
2 for his lobbying on behalf of Qatar to succeed.

3 89. As Defendant Muzin later admitted: “Broidy’s name comes up
4 in Embassy meetings often.” He also admitted, “I definitely identified him as
5 somebody who, was not, didn’t like them too much.” Defendant Muzin also
6 stated: “There’s no question I had conversations with them [the Qataris] about
7 Elliott.”

8 90. The efforts undertaken in September and October 2017 by
9 Defendant Muzin, acting as the agent of the State of Qatar, to influence the
10 United States Jewish community were manifestly unsuccessful. As alleged
11 above, by and large, American Jewish leaders declined to meet with the Emir
12 of Qatar when he was at the United Nations and declined offers of all-
13 expenses-paid trips to visit Qatar. Notwithstanding Muzin’s lack of success,
14 the State of Qatar nevertheless raised his monthly payment to \$300,000 a
15 month in November 2017 – shortly before the attacks on Plaintiffs began. On
16 information and belief, the increase in Muzin’s monthly pay was necessary to
17 support activities related to the hacks for which Muzin had responsibility.

18 91. Although Plaintiff Broidy was not the only outspoken critic of
19 the State of Qatar and of Muzin’s efforts on its behalf, on information and
20 belief, Defendants the State of Qatar, Al Thani, Al-Rumaihi, Stonington, and
21 Muzin, targeted Plaintiff Broidy specifically because he had exercised his
22 right to speak out on an issue of national and international concern and by
23 doing so, had negatively impacted Qatar’s interests.

24 92. Thereafter, the Qatari Defendants and the Agent Defendants
25 agreed to engage in and did in fact engage in or coordinate a series of hacks
26 and/or other misappropriation of the private communications, documents,
27

1 trade secrets and intellectual property of Plaintiffs, and unlawfully distributed
2 those materials to the media.

3 **V. DEFENDANTS EXECUTED A SOPHISTICATED**
4 **CYBERATTACK ON PLAINTIFFS**

5 **A. Defendants Unlawfully Accessed Plaintiffs' Computer Network,**
6 **Private Communications, Documents, Trade Secrets And**
7 **Intellectual Property**

8 93. On information and belief, sometime prior to December 27,
9 2017, Defendant State of Qatar acting directly or through the Agent
10 Defendants, retained the GRA Defendants to coordinate an offensive cyber
11 and information operation against Plaintiffs, including by infiltrating
12 Plaintiffs' computer networks in Los Angeles, California and obtaining
13 unauthorized access to Google email accounts of United States persons
14 associated with Plaintiffs. Servers hosting those accounts are located in
15 California.

16 94. On information and belief, the GRA Defendants introduced
17 Defendant State of Qatar to known and unknown threat actors to execute the
18 attacks, and supervised this work and were responsible for the overall
19 execution of the project.

20 95. Approximately one month before the cyberattacks against
21 Plaintiffs and their associates began, on information and belief, in October
22 2017 the GRA Defendants also opened a subsidiary of GRA organized under
23 the laws of Gibraltar and physically located in Doha, Qatar.

24 96. On information and belief, the GRA Defendants were actively
25 recruiting new employees within the small community of former U.S.
26 government offensive cyber operatives, and the GRA Defendants made it
27 clear within that community that they had been retained to conduct or
28 coordinate offensive cyber operations on behalf of Defendant State of Qatar.

1. The Rosenzweig Attack

1 97. Robin Rosenzweig, a U.S. citizen, serves as legal counsel to
2 Plaintiffs and lives in Los Angeles. On information and belief, Ms.
3 Rosenzweig has an email account through Gmail, an email service provided
4 by Google LLC (“Google”), a company headquartered in Mountain View,
5 California. Ms. Rosenzweig’s Gmail account contains private
6 communications and requires at least a username and password for access.

7 98. On December 27, 2017, Ms. Rosenzweig received an email at her
8 Gmail account that appeared to be an account security alert from Google. On
9 information and belief, the email used Google trademarks without the
10 permission of Google, including the Google logo and the Gmail logo. The
11 email was sent from a Gmail address, which had been disguised to look like
12 an authentic security alert from Google. The email purported to alert Ms.
13 Rosenzweig that the security on her account had been compromised and that
14 she needed to verify or change her account credentials. When she clicked on
15 the link in the email it directed her to a TinyURL website that appeared as if it
16 was an authentic Google account login page. TinyURL is a redirecting
17 service that provides shortened URLs that redirects a website visitor to the
18 website associated with the longer URL. It is known to be used by hackers
19 and scammers to avoid detection and circumvent spam and malware filters.
20 The URL address for that page was <http://tinyurl.com/yaw4jmpn>. When the
21 TinyURL link was clicked it redirected Ms. Rosenzweig to the following
22 website that contained Google’s logo and appeared to be an authentic Google
23 account update page: [https://mailchallenge-service-userupdate-myprofile-](https://mailchallenge-service-userupdate-myprofile-authsupport-key.userupdate.info/m/pn?tR0Il12=cHpXbG8yeXhyR0lOTTIxdW5KamhMMjln&nrm=SHo5dm5KNHREYVdpbkpFNQ==&cr=SkQ9PQ==&lan=en&rD3c)
24 [authsupport-](https://mailchallenge-service-userupdate-myprofile-authsupport-key.userupdate.info/m/pn?tR0Il12=cHpXbG8yeXhyR0lOTTIxdW5KamhMMjln&nrm=SHo5dm5KNHREYVdpbkpFNQ==&cr=SkQ9PQ==&lan=en&rD3c)
25 [key.userupdate.info/m/pn?tR0Il12=cHpXbG8yeXhyR0lOTTIxdW5KamhMM](https://mailchallenge-service-userupdate-myprofile-authsupport-key.userupdate.info/m/pn?tR0Il12=cHpXbG8yeXhyR0lOTTIxdW5KamhMMjln&nrm=SHo5dm5KNHREYVdpbkpFNQ==&cr=SkQ9PQ==&lan=en&rD3c)
26 [jln&nrm=SHo5dm5KNHREYVdpbkpFNQ==&cr=SkQ9PQ==&lan=en&rD3c](https://mailchallenge-service-userupdate-myprofile-authsupport-key.userupdate.info/m/pn?tR0Il12=cHpXbG8yeXhyR0lOTTIxdW5KamhMMjln&nrm=SHo5dm5KNHREYVdpbkpFNQ==&cr=SkQ9PQ==&lan=en&rD3c)
27

1 In=&rCv=WGxiZFh2YmRYd3Bt&VrCe2Ph=1&VrCe2Em=. However, that
2 page was a fraudulent login page that is no longer active. The TinyURL link
3 has been terminated by TinyURL for being used for spam, fraud, malware, or
4 other illegal activity.

5 99. On information and belief, that email was a spearphishing email
6 designed to gain unauthorized access to Ms. Rosenzweig's Google accounts
7 which include the full suite of Google's online products, such as Gmail,
8 Google Drive, Google Calendar, Google Contacts, and YouTube. Those
9 accounts contained, among other things, personal emails, business emails,
10 usernames and passwords to access other non-Google accounts belonging to
11 Ms. Rosenzweig, including an account on the computer network of Plaintiff
12 BCM. Without authorization and in violation of Google's Terms of Service,
13 the Defendant attackers used Ms. Rosenzweig's credentials to unlawfully
14 access passwords stored by Ms. Rosenzweig on Google's servers. Gmail
15 Program Policies and Google's Terms of Service, which are expressly
16 governed by the laws of California, prohibit illegal uses as well as sending
17 unauthorized email of any person without their consent.

18 100. On information and belief, Ms. Rosenzweig's Gmail account was
19 accessed and modified unlawfully and without her consent on or around
20 January 3, 2018. The Defendant attackers modified Ms. Rosenzweig's email
21 account settings so that emails containing "Mail.ru," "viewed," or "alert" were
22 marked as read and moved immediately to her trash. The Defendant attackers
23 did this to ensure that any legitimate security alerts would not be viewed by
24 Ms. Rosenzweig. Mail.ru is a Russian email service that publishes an app that
25 can be used to send and receive emails on Mail.ru or other email services like
26 Gmail. Unbeknownst to Ms. Rosenzweig, on January 4, 2018, Ms.
27 Rosenzweig received a true security alert – that went directly to her trash –

1 notifying her that a user or users of the Mail.ru app had obtained access to
2 read, send, delete, and manage Ms. Rosenzweig's Gmail account, all without
3 her awareness or consent.

4 2. The Mowbray Attack

5 101. Joel Mowbray is a U.S. citizen and resident of New York, New
6 York. Prior to December 27, 2017, Mr. Mowbray was known by Defendants
7 to be an associate of Plaintiff Broidy as well as a critic of both the Defendant
8 State of Qatar and Defendant Muzin.

9 102. On information and belief, Mr. Mowbray has a private Gmail
10 account that he uses to send and receive personal and business emails. Mr.
11 Mowbray's Gmail account contains private communications and requires at
12 least a username and password for access. Beginning on or around December
13 27, 2017, the same day as Ms. Rosenzweig was attacked, Mr. Mowbray also
14 began to receive a barrage of spearphishing emails disguised as Google News
15 stories that bore Google trademarks used without Google's permission and
16 were sent through Google's Gmail service in violation of Google's Terms of
17 Service and Gmail's Program Policies. The spearphishing, news-alert emails
18 contained links purportedly to news stories about Mr. Mowbray's family,
19 discrete projects on which Mr. Mowbray previously worked, and Plaintiff
20 Broidy. These topics were not the subject of general public awareness but
21 they, and their importance to Mr. Mowbray, were known to Defendant Muzin.

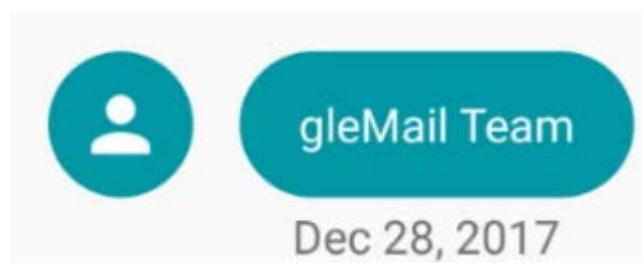
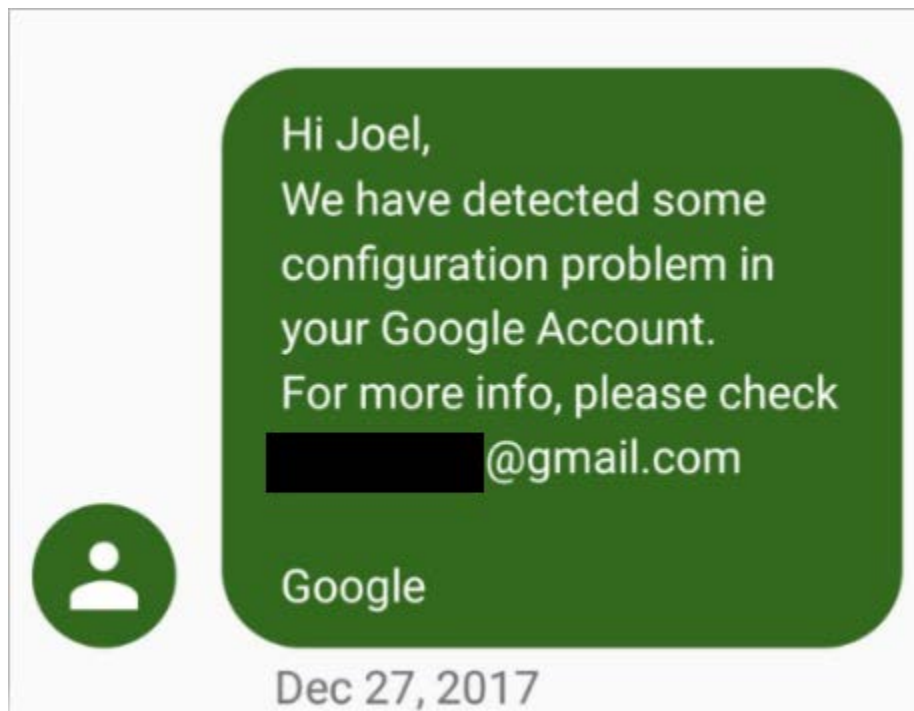
22 103. On information and belief, when Mr. Mowbray clicked on the
23 link in one of the news stories, it directed him to a shortened URL website,
24 like TinyURL or Bitly, that appeared as if it was an authentic Google account
25 login page. For example, one of the URL addresses was
26 <https://tinyurl.com/yckx3cny>. When this TinyURL link was clicked, it
27 redirected Mr. Mowbray to a website that asked for his Google login

1 credentials. Mr. Mowbray provided his credentials to at least one of these
2 malicious websites that contained Google's trademarks without the permission
3 of Google. TinyURL has now terminated this website because it has been
4 used for spam, fraud, malware, or other illegal activity.

5 104. On information and belief, Mr. Mowbray had two-factor
6 authentication enabled for his Google account on or about December 27,
7 2017. Two-factor authentication is an extra layer of security that requires not
8 only a password and username for login, but also something that only that user
9 has available to them, such as a mobile phone or other email address. Mr.
10 Mowbray's second factor was his mobile phone, which he had set to receive
11 verification text messages or a phone call from Google containing a
12 verification code.

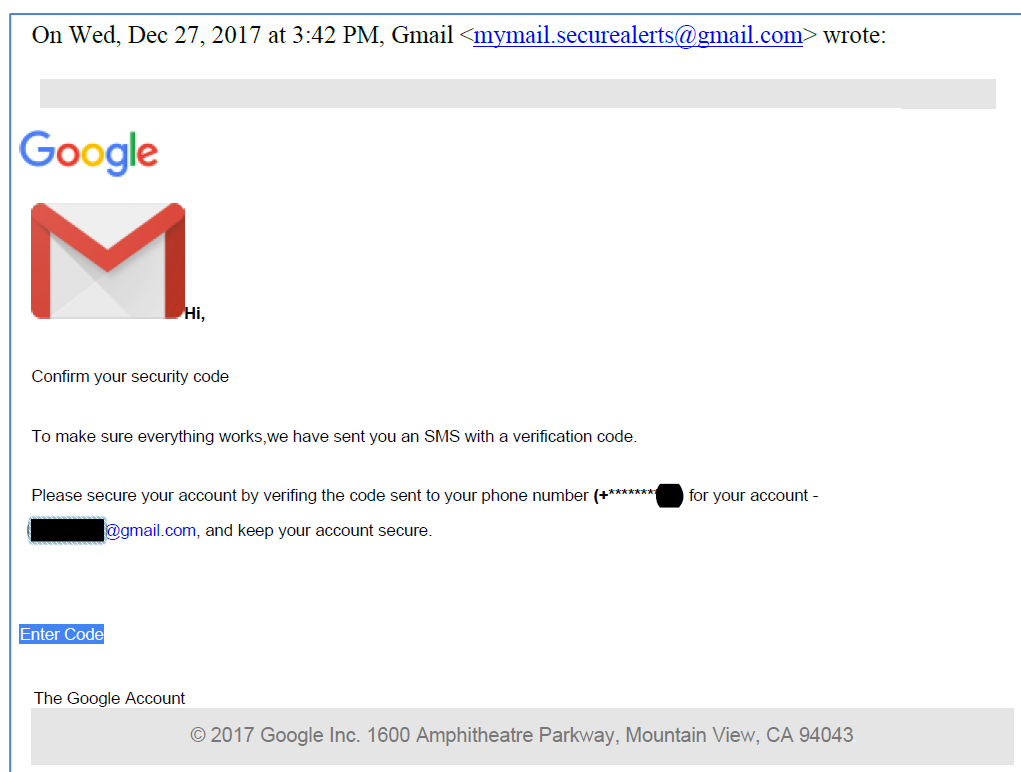
13 105. Beginning on or about December 27, 2017, Mr. Mowbray
14 received a call from a United States telephone number purportedly associated
15 with Google and containing a recording providing the verification code for his
16 account. Contemporaneous with that call from Google, Mr. Mowbray also
17 received from the Defendants several spearphishing text messages and calls
18 from U.S. phone numbers that were purportedly from Google. These phone
19 numbers are associated with U.S. phone carriers such as Hook Mobile. These
20 text messages and calls directed Mr. Mowbray to log in to his Gmail account
21 so that he could verify his account. Mr. Mowbray also received spearphishing
22 text messages such as those pictured below, and phone calls from phone
23 numbers with U.S. area codes and registered to U.S. carriers, such as Hook
24 Mobile, which mimicked two-factor authentication messages and made the
25 phishing emails appear authentic.

BOIES SCHILLER FLEXNER LLP



106. The Defendant attackers sent Mr. Mowbray these messages because they could not access his Google account without his two-factor authentication code.

107. On information and belief, Defendants also sent emails to Mr. Mowbray to obtain his two-factor authentication code. These emails, such as the one pictured below, were sent from a misleading Gmail account with the name “Gmail” and email addresses, such as mymail.securealerts@gmail.com and noreply.secureservicealerts@gmail.com, which were designed to appear as if they were from authentic Google security accounts. These emails used Google trademarks and logos without the permission of Google.



108. These spearphishing emails were designed to lure Mr. Mowbray to a malicious website seeking his Google login credentials. For example, one of the links went to a Bitly URL address: <http://bit.ly/2lber5Z>. If the Bitly link had been clicked, it would have redirected Mr. Mowbray to the following website that contained Google’s logo and appeared to be an authentic Google account page at the same domain (userupdate.info) as one of the spearphishing emails that Ms. Rosenzweig received seeking her Google login information:

1 [https://authsupport-myprofilelogon-servicemail-userowavalue-
key.userupdate.info/m/vc/?tR0II12=bnpFZ28zcXZwelNOTTIxdW5KamhM
Mjln&nrn=Vk49PQ==&cr=SkQ9PQ==&lan=en&rD3cIn=&rCv=WGxiZFh2
YmRYd3A0&VrCe2Ph=&VrCe2Em](https://authsupport-myprofilelogon-servicemail-userowavalue-
2 key.userupdate.info/m/vc/?tR0II12=bnpFZ28zcXZwelNOTTIxdW5KamhM
3 Mjln&nrn=Vk49PQ==&cr=SkQ9PQ==&lan=en&rD3cIn=&rCv=WGxiZFh2
4 YmRYd3A0&VrCe2Ph=&VrCe2Em). As with Ms. Rosenzweig, this link led
5 to a fraudulent login page that is no longer active. The Bitly link was created
6 on December 27, 2017, which is contemporaneous with the email that Mr.
7 Mowbray received. This Bitly link has been terminated by Bitly for
8 suspicious activity.

9 3. The Executive Assistant Attack

10 109. Plaintiff Broidy's Executive Assistant ("the Executive
11 Assistant") is a U.S. citizen and resident of Los Angeles, CA. She is an
12 employee of Plaintiff BCM. She has a private Gmail account that she uses to
13 send and receive personal emails. Her Gmail account contains private
14 communications and requires at least a username and password for access.

15 110. On information and belief, on or around January 14, 2018, just
16 weeks after Ms. Rosenzweig and Mr. Mowbray were attacked, the Executive
17 Assistant began to receive spearphishing emails disguised as Google security
18 alerts, which bore Google trademarks used without Google's permission and
19 were sent through Google's Gmail service in violation of Google's Terms of
20 Service and Gmail's Program Policies.

21 111. On information and belief, one of the spearphishing emails
22 contained a fictitious security alert with a picture of her face and part of her
23 phone number. The email was sent from a misleading Gmail account with the
24 name "Gmail Account" and the email address
25 noreply.user.secure.services@gmail.com, which had been drafted to look like
26 an authentic security alert from Google. The email purported to alert the
27 Executive Assistant that the security on her account had been compromised

1 and that she needed to verify or change her Google credentials. When she
2 clicked on the link in the email, it directed her to an Owly address, which
3 redirected her to a website that appeared as if it was an authentic Google
4 account login page. Like TinyURL and Bitly, Owly is a redirecting service
5 that provides shortened URLs that redirect a website visitor to the website
6 associated with the longer URL. It is known to be used by hackers and
7 scammers to avoid detection and circumvent spam and malware filters. The
8 URL address for that page was <http://ow.ly/FJZ030hLxof>. When the Owly
9 link was clicked, it redirected her to the following website that contains
10 Google's logo and appeared to be an authentic Google account login page:
11 <http://loms.96.lt/BDHRov58?platform=hootsuite>. However, that page was a
12 fraudulent login page that is no longer active.



Verify your security code

[Redacted]@gmail.com

To make sure everything works, we have sent you a SMS with a verification code.

Please secure your account [Redacted]@gmail.com by verifying the code sent to
your phone number [Redacted] and keep your account secure.

Verify

All the changes in your services will be alerted and verified with you.

The Help Center

© 2018 Google Inc., 1600 Mountain View, Amphitheatre Parkway, CA 94043, US

4. The BCM Attack

112. Plaintiff BCM has an exchange server physically located in Los Angeles, California. The server allows BCM employees to send and receive business and occasional personal emails. Plaintiff Broidy, his Executive Assistant, and several other employees all have secure email accounts on the BCM server containing private communications that require at least a username and password for access.

113. On information and belief, efforts to gain access to Plaintiff BCM's network appear to have commenced as early as January 7, 2018. The first successful access was gained on January 16, 2018, just two days after the successful spearphishing campaign on Plaintiff Broidy's Executive Assistant. The Defendant attackers maintained unauthorized and unlawful access to the BCM email server until at least February 25, 2018. During this period, there were thousands instances of unlawful and unauthorized access to corporate email accounts at Plaintiff BCM, including but not limited to unlawful and unauthorized connections to Plaintiff Broidy and his Executive Assistant's email accounts at Plaintiff BCM.

114. From January 7, 2018 to February 25, 2018, several instances of unlawful and unauthorized access occurred through Virtual Private Networks ("VPNs") that masked the IP addresses from which the attacks originated. VPNs route internet communication through additional networks to hide the original source of the connection. Some of these VPN connections occurred via IP addresses that are allocated to United States companies that lease them to third parties. For example, one of the suspicious IP addresses associated with the intrusions into the BCM server was leased from Micfo LLC, a company headquartered in Charleston, South Carolina.

115. On February 14, 2018 and February 19, 2018, unlawful and unauthorized connections originated from an IP address in Qatar. These two unlawful and unauthorized intrusions into BCM's California email server were not masked by VPNs, even though the connections immediately before and immediately after the access were routed through VPNs, possibly because the VPN failed or because the accessing computer automatically connected to Plaintiff BCM's network before the VPN could be activated. These connections revealed the actual location of a computer or computers accessing Plaintiff BCM's network from an IP address in Qatar.

116. These attacks resemble known international attacks by sophisticated cyber-hackers. Previous attacks against other victims by these same threat actors have involved similar fraudulent news alerts, malicious Google login pages, email addresses designed to resemble legitimate Google security addresses, fraudulent two-factor authentication messages, and the use of Mail.ru to control victims' accounts. In addition, one of the IP addresses used by the Defendants to access Plaintiffs' servers without authorization has been observed in other known, international attacks by these threat actors.

VI. DEFENDANTS EXECUTED A DISINFORMATION CAMPAIGN AGAINST PLAINTIFF BROIDY BY DISSEMINATING THE MATERIALS STOLEN FROM PLAINTIFFS

117. After unlawfully obtaining Plaintiffs' private communications, emails, documents and intellectual property, the Defendants viewed the stolen documents in an email application on their computers and converted them to PDFs for dissemination to third parties. In multiple instances, this conversion process resulted in information from the Defendants' computers being transferred as metadata to the PDF documents that were subsequently disseminated to third parties. Many of the PDFs disseminated to third parties contained time stamps different from the Pacific Time Zone associated with

1 the original documents – and instead bear time stamps from the Central and
2 Eastern Time Zones.

3 118. Upon information and belief, some of the unlawfully obtained
4 documents were given to United States media outlets in hard-copy form by
5 hand-delivery within the United States.

6 119. On February 24, 2018, Defendants registered the email address
7 “LA.Confidential@mail.com” through the company 1&1 Internet, Inc., which
8 operates in the United States through offices in Chesterbrook, Pennsylvania.
9 Mail.com provides free email addresses akin to Google’s Gmail service. On
10 or around March 1, 2018, Defendants used this address to unlawfully
11 distribute Plaintiffs’ stolen emails to a United States journalist employed by a
12 United States-based company.

13 120. On information and belief, Plaintiffs’ stolen emails have also
14 appeared on a website hosted by a United States company, GoDaddy LLC
15 (“GoDaddy”), which is headquartered in Scottsdale, Arizona. GoDaddy is a
16 domain registrar and web hosting service that sells website domains to users
17 so they may create their own webpage and hosts websites. Defendants further
18 obfuscated their identity using a registration masking service, Domain by
19 Proxy LLC, which allows a user to replace their own personal information
20 with information belonging to Domain by Proxy LLC for purposes of
21 registration. Domain by Proxy LLC is a company owned by GoDaddy LLC.

22 121. On March 1, 2018, the contents of emails stolen from Plaintiffs’
23 California-based computer accounts and servers appeared in the *Wall Street*
24 *Journal* in an article titled, “Trump Ally Was in Talks to Earn Millions in
25 Effort to End 1MDB Probe in U.S.” Additional emails stolen from those
26 California computer accounts and servers were published or reported on in
27

1 other media outlets including the *Huffington Post* on March 2, 2018 and the
2 *New York Times* on March 3, 2018 and the BBC on March 5, 2018.

3 122. On March 8, 2018, Defendant Muzin demonstrated his
4 knowledge that Plaintiff Broidy had been successfully targeted by the State of
5 Qatar by stating: “I did not cause the Broidy stuff, just because I have
6 information” and “I don’t know all the details, but I know that I am hearing
7 repeatedly that there’s a lot more coming.”

8 123. On March 22, 2018, the *New York Times* published a front page
9 article noting that an “anonymous group critical of Mr. Broidy’s advocacy of
10 American foreign policies in the Middle East” has been distributing
11 “documents, which included emails, business proposals and contracts,”
12 supposedly belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published
13 an article about Plaintiff Broidy, which noted that it had “received two
14 separate documents this week purporting to be versions” of materials
15 belonging to Plaintiff Broidy.

16 124. On March 26, 2018, the *New York Times* published another front
17 page story on Plaintiff Broidy that again acknowledged that it relied on
18 “[h]undreds of pages of Mr. Broidy’s emails, proposals and contracts”
19 received from “an anonymous group critical of Mr. Broidy’s advocacy of
20 American foreign policies in the Middle East.”

21 125. Media outlets in the United States and abroad continue to publish
22 – and to threaten to publish – materials stolen from Plaintiffs. Plaintiffs
23 continue to receive numerous press inquiries concerning such materials.

24 126. On information and belief, the State of Qatar, acting through the
25 Agent Defendants, was responsible for disseminating the emails and
26 documents stolen from Plaintiffs’ California-based email accounts and
27 servers.

1 127. On March 19, 2018, Plaintiffs, through counsel, formally
2 requested that the State of Qatar take appropriate action to halt the attacks on
3 Plaintiffs' emails, documents, and data, to stop Defendants from
4 disseminating Plaintiffs' emails, documents, and data, and/or to assist
5 Plaintiffs in halting dissemination if the hack had been conducted by a rogue
6 agent of the State of Qatar. However, to date, no response has been received
7 to that letter.

8 128. On information and belief, the Qatari Defendants, the GRA
9 Defendants and the Agent Defendants, while in the United States, conspired to
10 unlawfully access Plaintiffs' private communications, documents, trade
11 secrets and intellectual property located in California, and to disseminate that
12 information to the media as retribution for Plaintiff Broidy's public and
13 private criticisms of Defendants State of Qatar and Muzin, including his
14 direct criticisms of the State of Qatar to the President of the United States.

15 129. Upon information and belief, the Qatari Defendants, the GRA
16 Defendants and the Agent Defendants also carried out that conspiracy and
17 unlawfully accessed Plaintiffs' private communications, documents, trade
18 secrets and intellectual property located in California, and further engaged in
19 distribution of that information to media outlets in both the United States and
20 abroad. Upon information and belief, many of the instances of unlawful
21 distribution of illegally obtained took place within the United States.

22 130. The actions of the Qatari Defendants, the GRA Defendants and
23 the Agent Defendants as alleged herein were specifically proscribed by law
24 and were not matters left to the discretion, choice or judgment of a sovereign
25 state.

B. Defendants Muzin and Stonington Implicated Themselves With Respect To The Dissemination Of Materials Unlawfully Obtained From Plaintiffs' Email Accounts And Servers

131. Upon information and belief, on January 28, 2018, prior to the first public disclosure in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter at *McClatchy*, a Washington D.C. publication focused on politics, emailed Defendant Muzin and commented to Defendant Muzin that it was “time to rock.”

132. Weider’s article, “GOP Leans on Rainmaker who Courts Controversy on Two Continents,” which appeared in *McClatchy* on February 7, 2018, discussed Plaintiff Broidy’s political activities in the United States and his business interests in Romania. The article did not mention either of Muzin’s clients at the time (Qatar and Albania). Indeed, the article did not mention the Middle East at all. There is no apparent connection between Wieder’s January 28th remark to Muzin (that it was “time to rock”) and the February 7th article.

133. On February 27, 2018, Defendant Muzin demonstrated further foreknowledge of press reports about Plaintiff Broidy based on illegally obtained information when he informed Mowbray that there were “reporters circulating around” to focus on issues relating to Plaintiff Broidy, the Middle East and George Nader. (In that same conversation, Defendant Muzin also referred to “all the shit” that he believed Plaintiff Broidy and Mowbray had “done to” him.)

134. The first published report of any alleged connection between Nader and Plaintiff Broidy did not occur until March 3, 2018. Unless Defendant Muzin possessed or knew about documents and information contained in documents unlawfully obtained from Plaintiffs’ servers, Muzin would not have been a position to know about the particular issues relating to

1 Plaintiff Broidy, the Middle East and Nader that were about to become the
2 focus of media attention.

3 135. On March 5, 2018, Defendant Muzin informed Mowbray that
4 there was “more stuff coming” from the *New York Times*.

5 136. In the same meeting with Mowbray, Defendant Muzin discussed
6 meetings he had with his client the State of Qatar while serving as a registered
7 agent of Qatar. Muzin told Mowbray: “Broidy’s name comes up in Embassy
8 meetings often” and “I definitely identified him as somebody who, was not,
9 didn’t like them too much.” Muzin further acknowledged that everyone he
10 “fingered” was “in danger.” He warned Mowbray that Mowbray and Plaintiff
11 Broidy needed “to be very careful,” that the State of Qatar is “going after
12 you,” and that “Honestly, I know they’re after you and Broidy.”

13 137. In the same meeting, when Mowbray accused Defendant Muzin
14 of targeting Plaintiff Broidy for the State of Qatar and assisting in the hacks
15 on Plaintiffs and attempted hacks on Mowbray, Muzin responded “I was
16 doing my job.” Somewhat belatedly, Muzin stated that he realized that he
17 needed “to be a little more careful” when he spoke to Mowbray.

18 138. On March 22, 2018, as foretold by Defendant Muzin on March
19 5th, the *New York Times* published a front page article noting that an
20 “anonymous group critical of Mr. Broidy’s advocacy of American foreign
21 policies in the Middle East” has been distributing “documents, which included
22 emails, business proposals and contracts,” supposedly belonging to Plaintiffs.
23 On March 23, 2018, *Bloomberg* published an article about Plaintiff Broidy
24 and noted that it had “received two separate documents this week purporting
25 to be versions” of documents belonging to Plaintiff Broidy. On March 26,
26 2018, the *New York Times* published another front page story on Plaintiff
27 Broidy that again acknowledged that it relied on “[h]undreds of pages of Mr.

1 Broidy's emails, proposals and contracts" received from "an anonymous
2 group critical of Mr. Broidy's advocacy of American foreign policies in the
3 Middle East."

4 139. The actions of the Agent Defendants, the GRA Defendants and
5 Defendants Al Thani and Al-Rumaihi described herein are not subject to
6 derivative sovereign immunity because, among other things, the State of Qatar
7 is not entitled to sovereign immunity. In addition, although the actions of the
8 Agent Defendants, the GRA Defendants and Defendants Al Thani and Al-
9 Rumaihi originated in a conspiracy with the State of Qatar, upon information
10 and belief, the State of Qatar left to the Agent Defendants, the GRA
11 Defendants and Defendants Al Thani and Al-Rumaihi discretion and choice as
12 to the manner in which they would carry out their parts of the unlawful
13 conspiracy. As such, for these and other reasons, they are not entitled to
14 derivative sovereign immunity for their conduct in furtherance of the
15 conspiracy.

16 **CAUSES OF ACTION**
17 **FOR A FIRST CAUSE OF ACTION AGAINST ALL**
18 **DEFENDANTS**

19 **Computer Fraud and Abuse Act**
20 **18 U.S.C. §§ 1030(a)(2)(C) & (a)(5)**

21 140. Plaintiffs incorporate and adopt by reference the allegations
22 contained in each and every preceding paragraph of this First Amended
23 Complaint.

24 141. On information and belief, Defendant the State of Qatar, by itself
25 and/or through the Agent Defendants and the GRA Defendants, accessed or
26 caused to be accessed Plaintiffs' servers, and emails and documents physically
27 located on those servers, at BCM's offices in Los Angeles, California, as well
28 as Google servers located in California, specifically by accessing or causing to

1 be accessed accounts associated with Plaintiff Broidy and other BCM
2 employees.

3 142. Said Defendants first compromised Rosenzweig's personal email
4 account by a targeted spearphishing email in December 2017, and thereafter,
5 beginning on or about January 16, 2018, and without authorization, accessed
6 BCM's servers, and emails and documents physically located on those
7 servers, including the accounts Plaintiff Broidy and other BCM employees.
8 Defendants acted with knowledge that they were accessing these accounts
9 without Plaintiffs' authorization.

10 143. Defendants engaged in deliberate spearphishing attacks on
11 Rosenzweig, Mowbray and Plaintiff Broidy's Executive Assistant (as well as
12 attempted spearphishing attacks on Mowbray) and used information gained
13 from the attacks on Rosenzweig and Plaintiff Broidy's Executive Assistant to
14 obtain unauthorized access to Plaintiffs' servers, and emails and documents
15 physically located on those servers located in Los Angeles, California.
16 Defendants also implemented identifiable obfuscation techniques to engage in
17 ultimately unsuccessful efforts to hide the origin of their spearphishing attacks
18 and unauthorized access to Plaintiffs' servers, and emails and documents
19 physically located on those servers and the servers of Google.

20 144. On information and belief, by engaging in this conduct,
21 Defendants accessed "protected computers," defined by 18 U.S.C.
22 § 1030(e)(2)(B) as computers "used in or affecting interstate or foreign
23 commerce or communication."

24 145. Upon information and belief, as a direct result of the actions of
25 Defendants, Plaintiffs suffered damage, including harm to the integrity or
26 availability of their California-based servers, and emails and documents
27 physically located on those servers.

1 146. On information and belief, as a direct result of the actions of
2 Defendants, Plaintiffs also suffered loss, including but not limited to the
3 investigation costs associated with identifying the cyber-attacks and repairing
4 the integrity of Plaintiffs' servers after the attacks, including by hiring forensic
5 investigators and data security experts, and attorneys, among other losses, in
6 an amount to be proven at trial, but in any event, in excess of \$5,000 and,
7 together with the other alleged damages, in excess of \$75,000, exclusive of
8 interest and costs.

9 147. Upon information and belief, Defendants intentionally caused
10 such damage to Plaintiffs.

11 148. Defendants' conduct has caused, and will continue to cause
12 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
13 increased risk of further theft, and an increased risk of harassment. Such
14 injury cannot be compensated by monetary damages. Plaintiffs accordingly
15 seek an injunction prohibiting Defendants from engaging in the conduct
16 described in the Cause of Action.

17 149. Plaintiffs further seek a declaration that Defendants' conduct as
18 described in this First Amended Complaint is a violation of this Cause of
19 Action.

20 **FOR A SECOND CAUSE OF ACTION AGAINST ALL**
21 **DEFENDANTS**

22 **California Comprehensive Computer Data Access and Fraud Act**
23 **Cal. Pen. Code § 502**

24 150. Plaintiffs incorporate and adopt by reference the allegations
25 contained in each and every preceding paragraph of this First Amended
26 Complaint.

27 151. On information and belief, Defendant the State of Qatar, acting
28 by itself and/or through the Agent Defendants, violated § 502(c)(2) by

1 knowingly accessing and without permission taking and making use of
2 programs, data, and files from Plaintiffs' and Google's computers, computer
3 systems or computer networks, all of which were located in California.

4 152. On information and belief, Defendants have violated § 502(c)(4)
5 by knowingly accessing and without permission altering Plaintiffs' data,
6 which resided in Plaintiffs' and Google's computers, computer systems or
7 computer networks, all of which were located in California.

8 153. On information and belief, Defendants have violated § 502(c)(6)
9 by knowingly and without permission providing or assisting in providing, a
10 means of accessing Plaintiffs' and Google's computers, computer systems or
11 computer networks, all of which were located in California.

12 154. On information and belief, Defendants have violated § 502(c)(7)
13 by knowingly and without permission accessing, or causing to be accessed,
14 Plaintiffs' and Google's computers, computer systems or computer networks,
15 all of which were located in California.

16 155. On information and belief, Defendants have violated § 502(c)(9)
17 by knowingly and without permission using the Internet domain name or
18 profile of another individual in connection with the sending of one or more
19 email messages and thereby damaging Plaintiffs' and Google's computers,
20 computer systems or computer networks, all of which were located in Los
21 Angeles, California.

22 156. On information and belief, Defendants knowingly and unlawfully
23 accessed or caused to be accessed computers, computer systems or computer
24 networks at Plaintiff BCM and Google, all of which were located in
25 California. Defendants knew that at the time that they did not have the
26 authorization to take such action. This knowledge is demonstrated by
27 Defendants' use of spearphishing attacks and attempted spearphishing attacks,

1 as well as identifiable obfuscation techniques in an attempt to hide the origin
2 of their cyber-attacks.

3 157. On information and belief, Defendants engaged in these actions
4 as part of a targeted attack on Plaintiff Broidy, who is an outspoken critic of
5 the Qatari government.

6 158. On information and belief, as a direct and proximate result of
7 Defendants' unlawful conduct, Plaintiffs have been damaged in an amount to
8 be proven at trial, but in any event, in excess of \$75,000 exclusive of interest
9 and costs, including but not limited to the investigation costs associated with
10 identifying the cyber-attacks; verifying the integrity of the computers,
11 computer systems or computer networks, computer programs and/or computer
12 data, and/or data; and repairing the integrity of Plaintiffs' computer systems
13 after the attack, including by hiring forensic investigators and data security
14 experts. Plaintiffs are also entitled to recover their attorneys' fees pursuant to
15 § 502(e).

16 159. Additionally, Defendants' actions were willful and malicious,
17 such that Plaintiffs are also entitled to punitive damages under § 502(e)(4).

18 160. Defendants' conduct has caused, and will continue to cause
19 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
20 increased risk of further theft, and an increased risk of harassment. Such
21 injury cannot be compensated by monetary damages. Plaintiffs accordingly
22 seek an injunction prohibiting Defendants from engaging in the conduct
23 described in the Cause of Action.

24 161. Plaintiffs further seek a declaration that Defendants' conduct as
25 described in this First Amended Complaint is a violation of this Cause of
26 Action.

**FOR A THIRD CAUSE OF ACTION AGAINST ALL
DEFENDANTS**

**Receipt and Possession of Stolen Property
in Violation of Cal. Pen. Code § 496**

162. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

163. On information and belief, Defendant the State of Qatar, acting by itself and/or through the Agent Defendants, received property, including private communications, documents, trade secrets and intellectual property housed on Plaintiffs' and Google's servers, and in emails and documents physically located on those servers, all of which were located in California, and were stolen from Plaintiffs in California or otherwise obtained from Plaintiffs in California in a manner that constitutes theft.

164. Upon information and belief, in at least some instances, Defendants were in the United States when they received or possessed the unlawfully obtained information.

165. Upon information and belief, at least some instances of the unlawful receipt and possession of Plaintiffs stolen information occurred in the United States.

166. On information and belief, as a result of Defendants' actions, Plaintiffs have been damaged in an amount to be proven at trial, but in any event, in excess of \$75,000, exclusive of interest and costs, and are entitled to treble damages, the costs of bringing this suit, and attorneys' fees under § 496(c).

167. Defendants' conduct has caused, and will continue to cause Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Such

1 injury cannot be compensated by monetary damages. Plaintiffs accordingly
2 seek an injunction prohibiting Defendants from engaging in the conduct
3 described in the Cause of Action.

4 168. Plaintiffs further seek a declaration that Defendants' conduct as
5 described in this First Amended Complaint is a violation of this Cause of
6 Action.

7 **FOR A FOURTH CAUSE OF ACTION AGAINST ALL**
8 **DEFENDANTS**

9 **Invasion of Privacy by Intrusion**
10 **Upon Seclusion**

11 169. Plaintiffs incorporate and adopt by reference the allegations
12 contained in each and every preceding paragraph of this First Amended
13 Complaint.

14 170. Plaintiffs have a legally protected privacy interest in their
15 personal information, including in information contained on Plaintiffs' and
16 Google's servers, and in emails and documents physically located on those
17 servers, all of which were located in California, and had a reasonable
18 expectation that their information would remain private. Plaintiffs' accounts
19 were password protected, and at no time did Plaintiffs provide those
20 passwords, or the contents of their emails, to the public.

21 171. On information and belief, Defendant the State of Qatar, acting
22 by itself and/or through the Agent Defendants, hacked, stole, doctored, and
23 disseminated to others the personal and private information of Plaintiffs.
24 Defendants clearly did so without permission and with deliberate intent to
25 access and obtain Plaintiffs' personal and private information. At no point did
26 Plaintiffs authorize Defendants to hack, steal, doctor, or disseminate their
27 personal and private information. Upon information and belief, at least some
28

1 of the unlawful disseminations of Plaintiffs' personal information occurred
2 completely within the United States

3 172. On information and belief, Defendants' intentional intrusion
4 upon Plaintiffs' seclusion was highly offensive to Plaintiffs and would be
5 unjustifiable and highly offensive to an ordinary, reasonable person.

6 173. The public disclosure of Plaintiffs' personal information has
7 caused, and will continue to cause, Plaintiffs injury, including reputational
8 harm, an increased risk of further theft, and an increased risk of harassment.

9 174. Plaintiffs will continue to suffer this injury as long as their
10 personal information is available to Defendants and, subsequently, to media
11 organizations and the world at large.

12 175. The public disclosure of Plaintiffs' personal information has also
13 caused them to suffer monetary damages, at an amount to be proven at trial,
14 but in any event, in excess of \$75,000, exclusive of interest and costs.
15 Because Defendants' actions are intolerable in a civilized community,
16 Plaintiffs also seek punitive damages.

17 176. Defendants' conduct has caused, and will continue to cause
18 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
19 increased risk of further theft, and an increased risk of harassment. Such
20 injury cannot be compensated by monetary damages. Plaintiffs accordingly
21 seek an injunction prohibiting Defendants from engaging in the conduct
22 described in the Cause of Action.

23 177. Plaintiffs further seek a declaration that Defendants' conduct as
24 described in this First Amended Complaint is a violation of this Cause of
25 Action.

FOR A FIFTH CAUSE OF ACTION AGAINST ALL
DEFENDANTS

Conversion

178. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

179. Plaintiffs had ownership of and the right to possess their property, including private communications, documents, trade secrets and intellectual property, all of which were located in California.

180. Defendant the State of Qatar, acting by itself and/or through the Agent Defendants, converted or disposed of Plaintiffs' property including the rights to that property, by unlawfully accessing, or at a minimum receiving that property, including private communications, documents, trade secrets and intellectual property with knowledge that it had been unlawfully taken, and disseminating them to the media in the United States and abroad.

181. Upon information and belief, some instances of unlawful access and theft of Plaintiffs' property occurred completely within the United States.

182. Upon information and belief, at least some of the unlawful receipt and dissemination of Plaintiffs' personal information occurred completely within the United States.

183. Plaintiffs did not provide permission to access, receive or disseminate their exclusive personal and private information.

184. The public disclosure of Plaintiffs' personal information has also caused them to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of \$75,000, exclusive of interest and costs.

185. Additionally, Defendants' actions were willful and malicious, such that Plaintiffs are also entitled to punitive damages.

1 186. Defendants' conduct has caused, and will continue to cause
2 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
3 increased risk of further theft, and an increased risk of harassment. Such
4 injury cannot be compensated by monetary damages. Plaintiffs accordingly
5 seek an injunction prohibiting Defendants from engaging in the conduct
6 described in the Cause of Action.

7 187. Plaintiffs further seek a declaration that Defendants' conduct as
8 described in this First Amended Complaint is a violation of this Cause of
9 Action.

10 **FOR A SIXTH CAUSE OF ACTION AGAINST ALL**
11 **DEFENDANTS**

12 **Stored Communications Act**
13 **18 U.S.C. §§ 2701-12**

14 188. Plaintiffs incorporate and adopt by reference the allegations
15 contained in each and every preceding paragraph of this First Amended
16 Complaint.

17 189. Plaintiffs are "persons" within the meaning of 18 U.S.C.
18 §§ 2510(6) and 2707(a).

19 190. Defendants willfully and intentionally accessed without
20 authorization a facility through which an electronic communication service is
21 provided, namely, BCM's computer systems, including its email servers, as
22 well as Google's servers, thereby obtaining access to wire or electronic
23 communications while they were in electronic storage in such systems, in
24 violation of 18 U.S.C. § 2701(a).

25 191. As a result of Defendants' willful and intentional violations,
26 Plaintiffs have suffered damages and, as provided for in 18 U.S.C. § 2707, are
27 entitled to an award of the greater of the actual damages suffered or the

1 statutory damages, punitive damages, attorneys' fees and other costs of this
2 action, and appropriate equitable relief.

3 192. Defendants' conduct has caused, and will continue to cause
4 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
5 increased risk of further theft, and an increased risk of harassment. Such
6 injury cannot be compensated by monetary damages. Plaintiffs accordingly
7 seek an injunction prohibiting Defendants from engaging in the conduct
8 described in the Cause of Action.

9 193. Plaintiffs further seek a declaration that Defendants' conduct as
10 described in this First Amended Complaint is a violation of this Cause of
11 Action.

12 **FOR A SEVENTH CAUSE OF ACTION AGAINST ALL**
13 **DEFENDANTS**

14 **Digital Millennium Copyright Act**
15 **17 U.S.C. § 1201 *et seq.***

16 194. Plaintiffs incorporate and adopt by reference the allegations
17 contained in each and every preceding paragraph of this First Amended
18 Complaint.

19 195. Plaintiffs' computer networks and files contained information
20 subject to protection under the copyright laws of the United States that were
21 illegally accessed by Defendants without authorization. These materials
22 included, but were not limited to, presentations, proprietary business plans and
23 proposals, and strategic correspondence.

24 196. Access to the copyrighted material contained on Plaintiffs'
25 computer networks and email accounts was controlled by technological
26 measures, including firewalls, antivirus software, and measures restricting
27 access to users with valid credentials and passwords.

1 197. Defendants conducted a targeted attack to circumvent these
2 technological measures by stealing usernames and passwords from authorized
3 users. Defendants sent spearphishing emails containing links to malicious
4 websites designed to trick users into providing usernames and passwords.
5 Defendants used the information they obtained from their spearphishing
6 attacks to gain unauthorized access to Plaintiffs' computer networks and email
7 accounts.

8 198. Defendants' conduct caused Plaintiffs significant damages,
9 including, but not limited to, damage resulting from harm to Plaintiffs'
10 computers, loss in the value of Plaintiffs' trade secrets and proprietary
11 business information, and harm to the business.

12 199. As a result, Plaintiffs are entitled to the greater of their actual
13 damages or statutory damages as provided by 17 U.S.C. § 1203, in an amount
14 to be proven at trial. Plaintiffs are further entitled to attorneys' fees and costs
15 as provided by 17 U.S.C. § 1203.

16 200. Defendants' conduct has caused, and will continue to cause
17 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
18 increased risk of further theft, and an increased risk of harassment. Such
19 injury cannot be compensated by monetary damages. Plaintiffs accordingly
20 seek an injunction prohibiting Defendants from engaging in the conduct
21 described in the Cause of Action.

22 201. Plaintiffs further seek a declaration that Defendants' conduct as
23 described in this First Amended Complaint is a violation of this Cause of
24 Action.

25 **FOR AN EIGHTH CAUSE OF ACTION AGAINST ALL**
26 **DEFENDANTS**

27 **California Uniform Trade Secrets Act**
Cal. Civ. Code § 3426 *et seq.*

1 202. Plaintiffs incorporate and adopt by reference the allegations
2 contained in each and every preceding paragraph of this First Amended
3 Complaint.

4 203. The California Uniform Trade Secrets Act (“CUTSA”), Cal. Civ.
5 Code § 3426 *et seq.*, prohibits the misappropriation of any “trade secret.”

6 204. Defendants misappropriated a “trade secret” as defined by the
7 CUTSA to include “information, including a formula, pattern, compilation,
8 program, device, method, technique, or process, that: (1) Derives independent
9 economic value, actual or potential, from not being generally known to the
10 public or to other persons who can obtain economic value from its disclosure
11 or use; and (2) Is the subject of efforts that are reasonable under the
12 circumstances to maintain its secrecy.” Cal. Civ. Code. § 3426.1(d).

13 205. The BCM server stored trade secrets including but not limited to
14 highly confidential business plans and proposals, research supporting those
15 plans and proposals including costs and service projections, information
16 concerning business strategies and opportunities, and contacts for important
17 business relationships. These trade secrets are of immense value to Plaintiffs.

18 206. Plaintiffs take and have taken reasonable measures to keep this
19 information secret. For example, Plaintiffs have always maintained their
20 information on secured servers that are protected by passwords, firewalls, and
21 antivirus software.

22 207. Plaintiffs’ trade secrets derive independent actual and potential
23 economic value from not being generally known or available to the public or
24 other persons who can obtain economic value from their disclosure or use.

25 208. Plaintiffs’ trade secrets have significant value, resulting from
26 significant investment of time and resources.

209. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

210. Defendants improperly disclosed Plaintiffs' trade secrets without Plaintiffs' consent when they widely disseminated those trade secrets to media organizations for publication and at the time of such disclosure, knew or had reason to know that the information disclosed consisted of trade secrets.

211. As a direct consequence of Defendants' misappropriation, Plaintiffs have suffered damages, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts, loss in the value of Plaintiffs' trade secrets and business information, and harm to Plaintiffs' business, in an amount to be proven at trial.

212. As a direct consequence of Defendants' unlawful misappropriation, Defendants have unjustly benefited from their possession of Plaintiffs' trade secrets.

213. In misappropriating Plaintiffs' trade secrets, Defendants acted willfully and maliciously. Plaintiffs are thus entitled to exemplary damages under Section 3426.3(c) of the Civil Code. Plaintiffs are also entitled to reasonable attorneys' fees and costs under Section 3426.4 of the Civil Code.

214. Defendants' conduct has caused, and will continue to cause Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in the conduct described in the Cause of Action.

1 215. Plaintiffs further seek a declaration that Defendants' conduct as
2 described in this First Amended Complaint is a violation of this Cause of
3 Action.

4 **FOR A NINTH CAUSE OF ACTION AGAINST ALL**
5 **DEFENDANTS**

6 **Misappropriation of Trade Secrets In Violation of the Defend Trade**
7 **Secrets Act**

8 **18 U.S.C. § 1836 *et seq.***

9 216. Plaintiffs incorporate and adopt by reference the allegations
10 contained in each and every preceding paragraph of this First Amended
11 Complaint.

12 217. The materials that Defendants stole from Plaintiffs' and Google's
13 computer systems include trade secrets within the meaning of 18 U.S.C. §
14 1839.

15 218. The BCM server stored trade secrets including but not limited to
16 highly confidential business plans and proposals, research supporting those
17 plans and proposals including costs and service projections, information
18 concerning business strategies and opportunities, and contacts for important
19 business relationships. These trade secrets are of immense value to Plaintiffs.

20 219. Plaintiffs take and have taken reasonable measures to keep this
21 information secret. For example, Plaintiffs have always maintained their
22 information on secured servers that are protected by passwords, firewalls, and
23 antivirus software.

24 220. Plaintiffs' trade secrets were related to products or services used
25 in, or intended for use in, interstate or foreign commerce.

26 221. Defendants acquired Plaintiffs' trade secrets knowing or having
27 reason to know that the trade secrets were acquired by improper means.
28 Defendants also disclosed, or aided in the disclosure of, the trade secrets on

1 multiple occasions by sharing those trade secrets with media organizations, as
2 discussed herein, while knowing or having reason to know that the trade
3 secrets were acquired by improper means.

4 222. As a direct consequence of Defendants' misappropriation,
5 Plaintiffs have suffered damages, which include, but are not limited to,
6 damage resulting from harm to Plaintiffs' computers and servers, loss in the
7 value of Plaintiffs' trade secrets and business information, and harm to
8 Plaintiffs' business, in an amount to be proven at trial.

9 223. Furthermore, as a direct consequence of Defendants' unlawful
10 misappropriation, Defendants have unjustly benefited from their possession of
11 Plaintiffs' trade secrets.

12 224. In misappropriating Plaintiffs' trade secrets, Defendants acted
13 willfully and maliciously. Plaintiffs are thus entitled to exemplary damages
14 under 18 U.S.C. § 1836(b)(3).

15 225. In misappropriating Plaintiffs' trade secrets, Defendants acted
16 willfully and maliciously. Plaintiffs are thus entitled to exemplary damages
17 and reasonable attorneys' fees under 18 U.S.C. § 1836(b)(3).

18 226. Defendants' conduct has caused, and will continue to cause
19 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
20 increased risk of further theft, and an increased risk of harassment. Such
21 injury cannot be compensated by monetary damages. Plaintiffs accordingly
22 seek an injunction prohibiting Defendants from engaging in the conduct
23 described in the Cause of Action.

24 227. Plaintiffs further seek a declaration that Defendants' conduct as
25 described in this First Amended Complaint is a violation of this Cause of
26 Action.

FOR A TENTH CAUSE OF ACTION AGAINST ALL
DEFENDANTS

Civil Conspiracy

228. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

229. On information and belief, Defendants willfully, intentionally, and knowingly agreed and conspired with each other and with others to engage in the wrongful conduct alleged herein, including but not limited to

- a. Intentionally accessing Plaintiffs' and Google's servers, and emails and documents physically located on those servers accounts without authorization and then stealing and/or doctoring Plaintiffs' data and emails, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) & (a)(5);
- b. Knowingly accessing or causing to be accessed, and without permission taking, altering, and making use of Plaintiffs' and Google's programs, data, and files from Plaintiffs' computers, computer systems or computer network, and/or knowingly and without permission providing or assisting in providing a means of accessing Plaintiffs' and Google's computers, computer systems or computer network, in violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502;
- c. Intentionally receiving stolen property, in violation of Cal. Pen. Code § 496;

- d. Invading Plaintiffs' reasonable privacy interests and then publicly disseminating Plaintiffs' private information in a manner that is highly offensive to a person of reasonable sensibilities;
- e. Taking and converting Plaintiffs' exclusive private and personal property without permission and with deliberate intent to access and obtain Plaintiffs' personal and private information;
- f. Willfully and intentionally accessing without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, and thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a);
- g. Accessing copyrighted material contained on Plaintiffs' computer networks and email controlled by technological measures, in violation of 17 U.S.C. § 1201 *et seq.*; and/or

230. Misappropriating Plaintiffs' trade secrets in violation of Cal Civ. Code § 3426 *et seq.* and 18 U.S.C. § 1836 *et seq.* On information and belief, Defendants performed the acts alleged pursuant to, and in furtherance of, their agreement and/or furthered the conspiracy by cooperating, encouraging, ratifying, and/or adopting the wrongful acts of others.

231. On information and belief, Defendants expressly or tacitly agreed to, at the very least:

- a. Devise and execute a scheme to access Plaintiffs' computers, computer systems or computer network without permission, and to take, convert, alter, obtain, and use Plaintiffs' property,

1 including private communications, documents, trade secrets
2 and intellectual property;

- 3 b. Transfer and then disseminate the stolen private data; and/or
4 c. Access, receive, and/or possess the stolen private information,
5 all with the intent to harm Plaintiff Broidy, a private United
6 States citizen residing in California.

7 232. On information and belief, Defendants, with full knowledge that
8 they were engaged in wrongful actions, deliberately accessed, received,
9 possessed, stored, and helped to disseminate Plaintiffs' stolen property,
10 including private communications, documents, trade secrets and intellectual
11 property.

12 233. On information and belief, Defendants also had meetings wherein
13 targeting Plaintiff Broidy was discussed.

14 234. On information and belief, Defendants' agreement was both
15 explicit and tacit. In particular, those Agent Defendants who were registered
16 agents of the State of Qatar under FARA, as well as unregistered agents of the
17 State of Qatar, were incentivized to do the bidding of the State of Qatar and
18 engage in any acts that would further the overall scheme.

19 235. Upon information and belief, the conspiracy was agreed to within
20 the United States, and at least one step in furtherance of the conspiracy
21 occurred within the United States.

22 236. On information and belief, Plaintiffs have been injured and have
23 suffered monetary damages as a result of Defendants' conspiratorial actions in
24 an amount to be proven at trial, but in any event, in excess of \$75,000,
25 exclusive of interest and costs.

26 237. Defendants' conduct has caused, and will continue to cause
27 Plaintiffs irreparable injury, including reputational harm, loss of goodwill, an
28

1 increased risk of further theft, and an increased risk of harassment. Such
2 injury cannot be compensated by monetary damages. Plaintiffs accordingly
3 seek an injunction prohibiting Defendants from engaging in the conduct
4 described in the Cause of Action.

5 238. Plaintiffs further seek a declaration that Defendants' conduct as
6 described in this First Amended Complaint is a violation of this Cause of
7 Action.

8 **REQUEST FOR RELIEF**

9
10 239. Plaintiffs repeat and re-allege the allegations contained in each
11 and every preceding paragraph of this Complaint.

12 240. Plaintiffs request that this Court order the following relief:

- 13 a. Grant judgment in favor of Plaintiffs and against
14 Defendants;
- 15 b. Declare that Defendants' conduct constitutes violations of
16 the statutes and common law cited herein;
- 17 c. Grant all appropriate injunctive relief;
- 18 d. Award Plaintiffs an appropriate amount in monetary
19 damages as determined at trial, including pre- and post-
20 judgment interest, and any treble damages to which
21 Plaintiffs are entitled under Cal. Pen. Code § 496;
- 22 e. Award Plaintiffs punitive damages under 18 U.S.C.
23 § 2707, 18 U.S.C. § 1836(b)(3), Cal. Civ. Code
24 § 3426.3(c), and Cal. Pen. Code § 502, as well as under
25 Plaintiffs' claims for invasion of privacy by intrusion upon
26 seclusion, and conversion;

- 1 f. Award Plaintiffs attorneys' fees and the costs of bringing
2 this action; and
3 g. Grant Plaintiffs such other relief as is just and appropriate.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all of the claims asserted in this Complaint so triable.

Dated: May 24, 2018

Respectfully submitted,

BOIES SCHILLER FLEXNER LLP

By: 

LEE S. WOŁOSKY

Counsel for Plaintiffs

BOIES SCHILLER FLEXNER LLP